

GBPPR 'Zine



Issue #122 / The Monthly Journal of the American Hacker / June 2014

"Who cares if six million Jews were exterminated?" asked the businessman back at the cafe, in a shocking endorsement of that reality. 'I don't care if they were turned into soap. What I care about is the salary I have lost, the never-ending taxes I am forced to pay, the criminals who rule this country, the anger I carry inside.'"

--- Excerpt from a Golden Dawn hit-piece by *The Guardian*. It appears that Greece (and Europe) is waking up, and guess who doesn't like that?

(theguardian.com/world/2014/jun/07/greece-golden-dawn-fascism-threat-to-democracy)

Table of Contents

- ◆ **Page 2 / SLC-96 Digital Line Preservice Tests**
 - ◆ Performing preservice tests on a SLC-96 digital line from the central office terminal to the remote terminal.
- ◆ **Page 22 / Motorola High Performance Data Overview**
 - ◆ General overview of Motorola's High Performance Data 700/800 MHz mobile data system.
- ◆ **Page 33 / GBPPR RAGEMASTER Experiments**
 - ◆ Experimental homebrew version of the NSA's RAGEMASTER VGA video RF retro-reflector.
- ◆ **Page 50 / Bonus**
 - ◆ Milwaukee Derp
- ◆ **Page 51 / The End**
 - ◆ Editorial and rants.

SLC-96 Digital Line Preservice Tests

BELL SYSTEM PRACTICES
AT&TCo Standard

SECTION 363-202-215
Issue 2, July 1981

“SLC”-96 SUBSCRIBER LOOP CARRIER SYSTEM DIGITAL LINE PRESERVICE TESTS DIGITAL SUBSCRIBER CARRIER SYSTEMS

This section provides procedures for performing preservice tests on a SLC-96 digital line from the central office terminal (COT) to the remote terminal (RT) using the ED7C351-30 LINE TEST ADAPTER to access the line at each location. When the LINE TEST ADAPTER is not available, Chart 3 provides procedures for performing preservice tests from the central office main distributing frame (CO MDF) to the last repeater or to the power looping repeater if the system is powered from the COT and RT. The methods for testing 238A, 239A, 208-, 209-, 217-, and 251-type repeaters prior to installing them in a digital line can be found in Section 363-201-225. Pair loss measurements and dc tests are provided in Section 640-527-220 when using the J98725AA Test Set or in Section 640-525-220 when using the 113A or 113B Test Set. The SLC-96 system is described in Section 363-202-100. Information on system number, cable pairs, RT location, and repeater locations can be found in the work print and SLC-96 System Facility Record.

This section is reissued to include the remote power feed terminal (RPFT) and the use of the new ED7C351-30 LINE TEST ADAPTER which plugs into the LINE INTERFACE UNIT (LIU) slots at the COT and RT to access the entire digital line being tested (Fig. 1). Since this is a general revision, arrows normally used to indicate changes have been omitted.

Charts 1 and 2 are the preferred methods of preservice testing the digital line since those procedures test the complete line and all wiring and cabling at the central office and remote terminal. Chart 3 only provides for testing from the main distributing frame (MDF) at the central office to the apparatus case closest to the remote terminal. The preservice tests in Chart 3 may be performed before the channel banks at either end of the system are installed. An alternate method of using Chart 3 is to access the digital line at the RT splice instead of at the last apparatus case. In order to access the digital line at the RT splice, the test equipment must be clipped onto the cable conductors. To connect directly to the cable conductors at the splice location closest to the RT channel bank, a Sierra 247A-1 cable splitting cord (Fig. 2) must be used with the Sierra 317B T1 Line and Repeater Test Set. To use the 417A-2 PCM Line and Repeater Test Set, a Sierra CO325600 adapter must be used along with the Sierra 247A-1 cable splitting cord. With this method of testing a power looping bidirectional repeater must be inserted in the 317B or 417A-2 test sets instead of using the repeater from the digital line as stated in Step 1 of Chart 3. All other steps in Chart 3 apply for testing from the central office MDF to the splice at the RT.

Prior to starting **terminal-to-terminal** installation tests of TOP 363-202-400 and 363-202-401, performance of all main and protection digital lines of each SLC-96 system should be checked.

When the media for a SLC-96 system is T1 digital lines (with standard or low power repeaters) terminating in T1 office repeater bays, the preservice tests are performed per Section 365-224-500 which is used for T1 trunk facilities.

If the digital lines are equipped with optional fault-locating filters, fault-locating tests will be performed in addition to the tests of this section. Fault-locating tests are performed using the procedures

*Trademark of Western Electric.

NOTICE

Not for use or disclosure outside the
Bell System except under written agreement

Printed in U.S.A.

Page 1

SLC-96 Digital Line Preservice Tests

SECTION 363-202-215

of Section 363-202-515 (passive filters) or 363-202-516 (active filters). Appropriate records of initial fault-locating tests should be retained for future reference.

CHART	PAGE
1 — Line Powered From COT Only Using Line Test Adapter (With or Without Remote Power Feed Terminal)	2
2 — Line Powered From COT and RT Using Line Test Adapter (With or Without Remote Power Feed Terminal)	5
3 — Testing Without Line Test Adapter	9

CHART 1

LINE POWERED FROM COT ONLY USING LINE TEST ADAPTER (WITH OR WITHOUT REMOTE POWER FEED TERMINAL)

APPARATUS:

At the Remote Terminal

- 1 — 602B Terminating Unit (Fig. 3)
- 1 — ED7C351-30 Line Test Adapter (Fig. 4)

At the Central Office Terminal

- 1 — 107B Power Unit (Fig. 5)
- 1 — ED7C351-30 Line Test Adapter

Note: If equivalent test equipment is used, the manufacturer's operation manual must be used.

STEP	PROCEDURE
	<i>At the RT</i>
1	Connect the 602B Terminating Unit to the LINE TEST ADAPTER as follows: <div style="text-align: center;"> <div style="display: inline-block; vertical-align: middle;"> From 602B SIDE 1 to LSI From 602B SIDE 2 to LSO </div> <div style="display: inline-block; vertical-align: middle; font-size: 2em;">}</div> <div style="display: inline-block; vertical-align: middle;">ONE CORD</div> </div>
2	Plug LINE TEST ADAPTER into LIU slot for digital line to be tested (Fig. 6). <p>Note: This loops the digital line back toward the COT. This is the only activity required at the RT to test the digital line.</p>

SLC-96 Digital Line Preservice Tests

ISS 2, SECTION 363-202-215

CHART 1 (Contd)

STEP	PROCEDURE
3	<p>If the remote power feed terminal (RPFT) is being used, ensure the RPFT is turned up. Refer to Section 363-202-525 for turn-up procedures.</p> <p>At the COT</p>
4	<p>Verify all patch cords are removed from the 107B and the AC switch on the 107B is in the OFF position.</p> <p>Danger: The 107B must produce a high dc voltage (+135 and -135 volts to ground) to power the repeatered line under test. It is designed to prevent high voltages on the patch cords until connections have been made to both the 107B jacks and the adapter test jacks. The double patch cord supplied with the 107B must be used to make these connections. Use of substitute cords defeats the safety features and may prevent the 107B from powering the line under test.</p>
5	<p>Using the special patch cord furnished with the 107B, connect the 107B to the LINE TEST ADAPTER as follows:</p> <p style="text-align: center;"> From 107B LSO to LSO } From 107B LSI to LSI } ONE CORD </p>
6	<p>Plug LINE TEST ADAPTER into LIU slot for digital line to be tested (Fig. 6).</p>
7	<p>Set the 107B LINE CURRENT switch to 60 mA position.</p> <p>Danger: The following steps place voltages of up to 300 volts dc on the cable pairs being tested. Verify that outside plant personnel are notified before continuing the tests.</p>
8	<p>Plug the 107B power cord into a convenient 117-Vac 60-Hz outlet, and operate the AC switch to the ON position.</p> <p>Requirement: The OUTPUT ON lamp lights.</p>
9	<p>Set the 107B meter switch to the V OUT position.</p> <p>Requirement: The meter indicates between 20 and 270 volts on the 0 to 320 volts scale.</p>
10	<p>Operate the meter switch to the -I position and note the meter indication.</p> <p>Requirement: The meter indicates between 50 and 70 mA.</p> <p>Note: No current reading indicates an open line or the digital line is connected to the wrong shelf.</p>

Page 3

SLC-96 Digital Line Preservice Tests

SECTION 363-202-215

CHART 1 (Contd)

STEP	PROCEDURE
11	<p>Operate the meter switch to the +I position and note the meter indication (lower scale).</p> <p>Requirement: The meter indication does not change more than one division (5 mA) from that of Step 10.</p> <p>Note: A difference in meter readings of more than 5 mA indicates a cable pair leakage to ground. Refer cable trouble to the proper work group.</p>
12	<p>Depress the TRANSMIT ERRORS button on the 107B.</p> <p>Requirement: The ERRORS lamp flashes repeatedly, indicating transmission around the loop line.</p> <p>Note: If this requirement is not met, check the test connections and test equipment, then refer to Section 363-202-515 or 363-202-516 for digital line trouble-locating information.</p>
13	<p>Insert a dummy plug into the 107B FL SIG jack.</p> <p>Requirement: The PULSES and ERRORS lamps remain extinguished while the dummy plug is in the FL SIG jack.</p>
14	<p>Remove the dummy plug from the FL SIG jack.</p> <p>Requirement: The PULSES lamp lights continuously, and the ERRORS lamp does not flash more than five times in any 30-second period.</p>
15	<p>Set the 107B POWER UNIT AC switch to the OFF position.</p>
16	<p>Unplug the power cord of the 107B from the 117-Vac outlet.</p>
17	<p>Repeat Steps 1 through 16 for all main and protection digital lines to be tested.</p>
18	<p>When testing is completed, remove all patch cord connections and notify RT personnel that testing is complete.</p>

SLC-96 Digital Line Preservice Tests

ISS 2, SECTION 363-202-215

CHART 2

LINE POWERED FROM COT AND RT USING LINE TEST ADAPTER (WITH OR WITHOUT REMOTE POWER FEED TERMINAL)

APPARATUS:

At the Remote Terminal

- 1 —107B Power Unit (Fig. 5)
- 1 —ED7C351-30 Line Test Adapter (Fig. 4)

At the Central Office Terminal

- 1 —107B Power Unit
- 1 —ED7C351-30 Line Test Adapter

Note: If equivalent test equipment is used, the manufacturer's operation manual must be used.

STEP

PROCEDURE

At the RT

- 1 Verify commercial ac power is available at the RT.
- 2 Verify all patch cords are removed from the 107B and the AC switch on the 107B is in the OFF position.

Danger: The 107B must produce a high dc voltage (+135 and -135 volts to ground) to power the repeatered line under test. It is designed to prevent high voltages on the patch cords until connections have been made to both the 107B jacks and the RT test jacks. The double patch cord supplied with the 107B must be used to make these connections. Use of substitute cords defeats the safety features and may prevent the 107B from powering the line under test.

- 3 Using the special patch cord furnished with the 107B, connect the 107B to the LINE TEST ADAPTER as follows:

From 107B LSO to LSO
From 107B LSI to LSI } ONE CORD

- 4 Plug the LINE TEST ADAPTER into the LIU slot for the digital line to be tested (Fig. 6).
- 5 Complete the following patch on the 107B:

From: FL SIG to RECEIVE DS1

Page 5

SLC-96 Digital Line Preservice Tests

SECTION 363-202-215

CHART 2 (Contd)

STEP	PROCEDURE
6	<p>Set the 107B LINE CURRENT switch to the 60 mA position.</p> <p>Danger: The following steps place voltages of up to 300 volts dc on the cable pairs being tested. Verify that outside plant personnel are notified before continuing the tests.</p>
7	<p>Plug the 107B power cord into a convenient 117-Vac 60-Hz outlet, and operate the AC switch to the ON position.</p> <p>Requirement: The OUTPUT ON lamp lights.</p>
8	<p>Set the 107B meter switch to the V OUT position.</p> <p>Requirement: The meter indicates between 20 and 270 volts on the 0 to 320 volts scale.</p>
9	<p>Set the meter switch to the -I position.</p> <p>Requirement: The meter indicates between 50 and 70 mA.</p> <p>Note: No current reading indicates an open line or the digital line is connected to the wrong shelf.</p>
10	<p>Set the meter switch to the +I position.</p> <p>Requirement: A meter change of not more than 5 mA from that of Step 9.</p> <p>Note: A difference in meter readings of more than 5 mA indicates a cable pair leakage to ground. Refer cable trouble to the proper work group.</p>
11	<p>The digital line under test is now looped back toward the COT. Advise CO personnel that the RT arrangements are complete.</p>
12	<p>If the remote power feed terminal (RPFT) is being used, ensure the RPFT terminal is turned up. Refer to Section 363-202-525 for turn-up procedures.</p>
13	<p>Verify all patch cords are removed from the 107B and the AC switch on the 107B is in the OFF position.</p> <p>Danger: The 107B must produce a high dc voltage (+135 and -135 volts to ground) to power the repeatered line under test. It is designed to prevent high voltages on the patch cords until connections have been made to both the 107B jacks</p>

SLC-96 Digital Line Preservice Tests

ISS 2, SECTION 363-202-215

CHART 2 (Contd)

STEP	PROCEDURE
	<p>and the adapter test jacks. The double patch cord supplied with the 107B must be used to make these connections. Use of substitute cords defeats the safety features and may prevent the 107B from powering the line under test.</p>
14	<p>Using the special patch cord furnished with the 107B, connect the 107B to the LINE TEST ADAPTER as follows:</p> <p style="text-align: center;"> From 107B LSO to LSO From 107B LSI to LSI } ONE CORD </p>
15	<p>Plug the LINE TEST ADAPTER into the LIU slot for the digital line to be tested (Fig. 6).</p>
16	<p>Set the 107B LINE CURRENT switch to the 60 mA position.</p> <p>Danger: The following steps place voltages of up to 300 volts dc on the cable pairs being tested. Verify that outside plant personnel are notified before continuing the tests.</p>
17	<p>Plug the 107B power cord into a convenient 117-Vac 60-Hz outlet, and operate the AC switch to the ON position.</p> <p>Requirement: The OUTPUT ON lamp lights.</p>
18	<p>Set the 107B meter switch to the V OUT position.</p> <p>Requirement: The meter indicates between 20 and 270 volts on the 0 to 320 volts scale.</p>
19	<p>Operate the meter switch to the -I position and note the meter indication.</p> <p>Requirement: The meter indicates between 50 and 70 mA.</p> <p>Note: No current reading indicates an open line or the digital line is connected to the wrong shelf.</p>
20	<p>Operate the meter switch to the +I position and note the meter indication (lower scale).</p> <p>Requirement: The meter indication does not change more than one division (5 mA) from that of Step 19.</p> <p>Note: A difference in meter readings of more than 5 mA indicates a cable pair leakage to ground. Refer cable trouble to the proper work group.</p>
21	<p>Depress the TRANSMIT ERRORS button on the 107B.</p>

Page 7

SLC-96 Digital Line Preservice Tests

SECTION 363-202-215

CHART 2 (Contd)

STEP	PROCEDURE
	<p>Requirement: The ERRORS lamp flashes repeatedly, indicating transmission around the looped line.</p> <p>Note: If this requirement is not met, check the test connections and test equipment, then refer to Section 363-202-515 or 363-202-516 for digital line trouble-locating information.</p>
22	<p>Insert a dummy plug into the 107B FL SIG jack.</p> <p>Requirement: The PULSES and ERRORS lamps remain extinguished while the dummy plug is in the FL SIG jack.</p>
23	<p>Remove the dummy plug from the FL SIG jack.</p> <p>Requirement: The PULSES lamp lights continuously, and the ERRORS lamp does not flash more than five times in any 30-second period.</p>
24	<p>Set the 107B POWER UNIT AC switch to the OFF position.</p>
25	<p>Unplug the power cord of the 107B from the 117-Vac outlet.</p>
26	<p>Repeat Steps 2 through 25 for all main and protection digital lines to be tested.</p>
27	<p>When testing is complete, remove all patch cord connections and notify RT personnel that testing is complete.</p>

SLC-96 Digital Line Preservice Tests

ISS 2, SECTION 363-202-215

CHART 3

TESTING WITHOUT LINE TEST ADAPTER

APPARATUS:

At the Last Repeater (or Power Looping Repeater)

- 1 —Sierra 317B T1 Line and Repeater Test Set
- 1 —Sierra 247A-1 Cable Splitting Adapter (Optional)

or

- 1 —Sierra 417A-2 PCM Line and Repeater Test Set
- 1 —Sierra 247A-1 Cable Splitting Adapter (Optional)
- 1 —Sierra CO325600 Adapter (Optional)

At the COT MDF

- 1 —107B Power Unit (Fig. 5)
- 1 —Cord, W6P, equipped with a safety grounding clip
- 1 —310-Type Dummy Plug
- 2 —MDF Test Cords, according to the type of frame protectors

FRAME TYPE	TEST CORD
444 Jack	P2CY
C50	P2DC
300	2P34A
302	W2GD
303	W2GM

STEP	PROCEDURE
------	-----------

At the Last Repeater (or Power Looping Repeater)

- | | |
|---|---|
| 1 | Remove the repeater from the digital line to be tested and insert it into the 317B or 417A-2 repeater slot. |
|---|---|

Page 9

SLC-96 Digital Line Preservice Tests

SECTION 363-202-215

CHART 3 (Contd)

STEP	PROCEDURE
	<p>Note 1: Verify that the proper adapter insert in the 317B or 417A-2 is being used for the type of repeater being tested.</p> <p>Note 2: When using the Sierra 247A-1 cable splitting cord, the green lead connects to the tip side and the white lead connects to the ring side of output pair of the digital line. The red lead connects to the tip side and the black lead connects to the ring side of the input pair of the digital line.</p>
2	<p>Insert the probe from the 317B or 417A-2 into the repeater slot from which the repeater was removed in Step 1.</p> <p>Note: Verify that the proper probe on the 317B or 417A-2 is being used for the type of repeater housing that you have.</p>
3	<p>Set the TERMINATION switch on the 317B or 417A-2 to the LOOP/FROG position and operate the POWER switch to ON.</p> <p>Note: The digital line to be tested is now looped back toward the CO.</p> <p>At Central Office MDF</p>
4	<p>Verify that all patch cords and power cords have been removed from the 107B and the 107B AC switch is in the OFF position.</p> <p>Danger: The 107B must produce a high dc voltage (+135 and -135 volts to ground) to power the repeatered line under test. It is designed to prevent high voltages on the patch cords until connections have been made to the 107B jacks and the safety grounding clip has been connected. The W6P patch cord must be used to make these connections. Use of substitute cords defeats the safety features and may prevent the 107B from powering the line under test.</p>
5	<p>Complete the following patch/test cord connections in the order given (see Fig. 7).</p>

CORD TYPE	FROM	TO
According to Frame Type	MDF Protector/Connector/Jack Side 1 of Digital Line Under Test	W6P Cord Side 1 (No safety grounding clip)
According to Frame Type	MDF Protector/Connector/Jack Side 2 of Digital Line Under Test	W6P Cord Side 2 (Attach safety grounding clip to adjacent framework ground)

SLC-96 Digital Line Preservice Tests

ISS 2, SECTION 363-202-215

CHART 3 (Contd)

STEP	PROCEDURE
	<p>Note 1: Side 2 of the W6P cord is equipped with a safety grounding clip which corresponds to the knurled side of the 474A plug on the other end of the cord.</p> <p>Note 2: Verify that the connections are as given in Step 5 and Fig. 7; otherwise, incorrect readings will result.</p>
6	<p>After the above connections are complete and have been checked, insert the 474A plug end of the W6P cord into the 107B LSI/LSO jacks, noting that the knurled side of the 474A plug is connected to the LSI jack.</p> <p>Danger: The following steps place voltages of up to 300 volts dc on the cable pairs being tested. Verify that outside plant personnel are notified before connecting the 107B power supply to the line under test.</p>
7	Set the 107B LINE CURRENT switch to the 60 mA position.
8	<p>Plug the 107B power cord into a convenient 117-Vac 60-Hz outlet; operate the meter switch to the V OUT position and place the AC switch to ON.</p> <p>Requirement 1: The OUTPUT ON lamp lights.</p> <p>Requirement 2: The meter indicates between 20 and 270 volts (0 to 320V scale).</p>
9	<p>Operate the meter switch to the -I position and note the meter indication.</p> <p>Requirement: The meter indicates between 50 and 70 mA.</p> <p>Note: No current reading indicates an open line.</p>
10	<p>Operate the meter switch to the +I position and note the meter indication (lower scale).</p> <p>Requirement: The meter indication does not change more than one division (5 mA) from that of Step 9.</p> <p>Note: A difference in meter readings of more than 5 mA indicates a cable pair leakage to ground. Refer cable trouble to the proper work group.</p>
11	<p>Depress the TRANSMIT ERRORS button on the 107B.</p> <p>Requirement: The ERRORS lamp flashes repeatedly, indicating transmission around the looped line.</p> <p>Note: If this requirement is not met, check the test connections and test equipment, then refer to Section 363-202-515 or 363-202-516 for digital line trouble-locating information.</p>

Page 11

SLC-96 Digital Line Preservice Tests

SECTION 363-202-215

CHART 3 (Contd)

STEP	PROCEDURE
12	Insert a dummy plug into the 107B FL SIG jack. Requirement: The PULSES and ERRORS lamps remain extinguished while the dummy plug is in the FL SIG jack.
13	Remove the dummy plug from the FL SIG jack. Requirement: The PULSES lamp lights continuously, and the ERRORS lamp does not flash more than five times in any 30-second period.
14	Set the 107B POWER UNIT AC switch to the OFF position.
15	Unplug the power cord of the 107B from the 117-Vac outlet.
16	Repeat Steps 1 through 15 for all main and protection digital lines to be tested.
17	When testing is completed, turn the 107B AC switch to the OFF position, and remove all connections at the MDF and at the last repeater location.

SLC-96 Digital Line Preservice Tests

ISS 2, SB

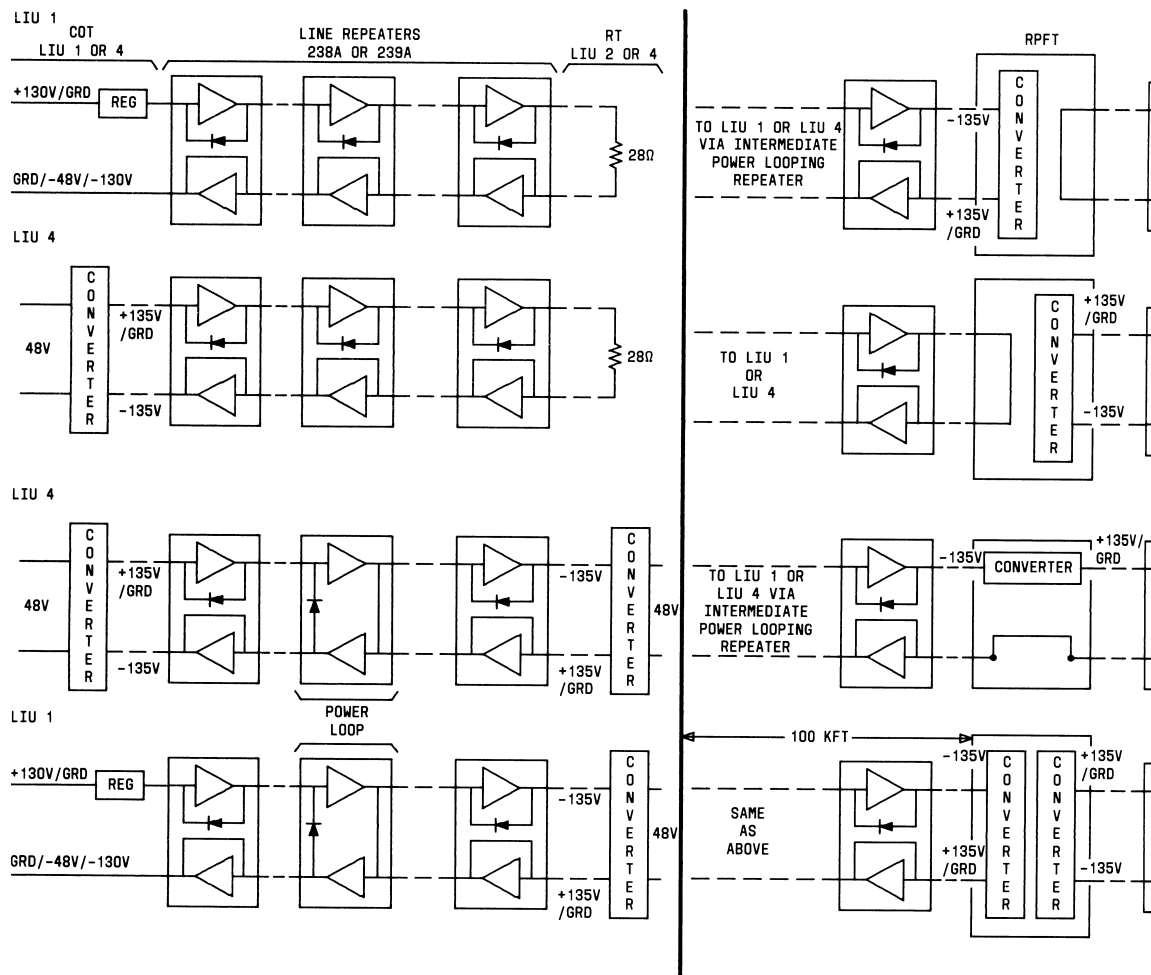


Fig. 1 — Typical SLC-96 Po

SLC-96 Digital Line Preservice Tests

ISS 2, SECTION 363-202-215

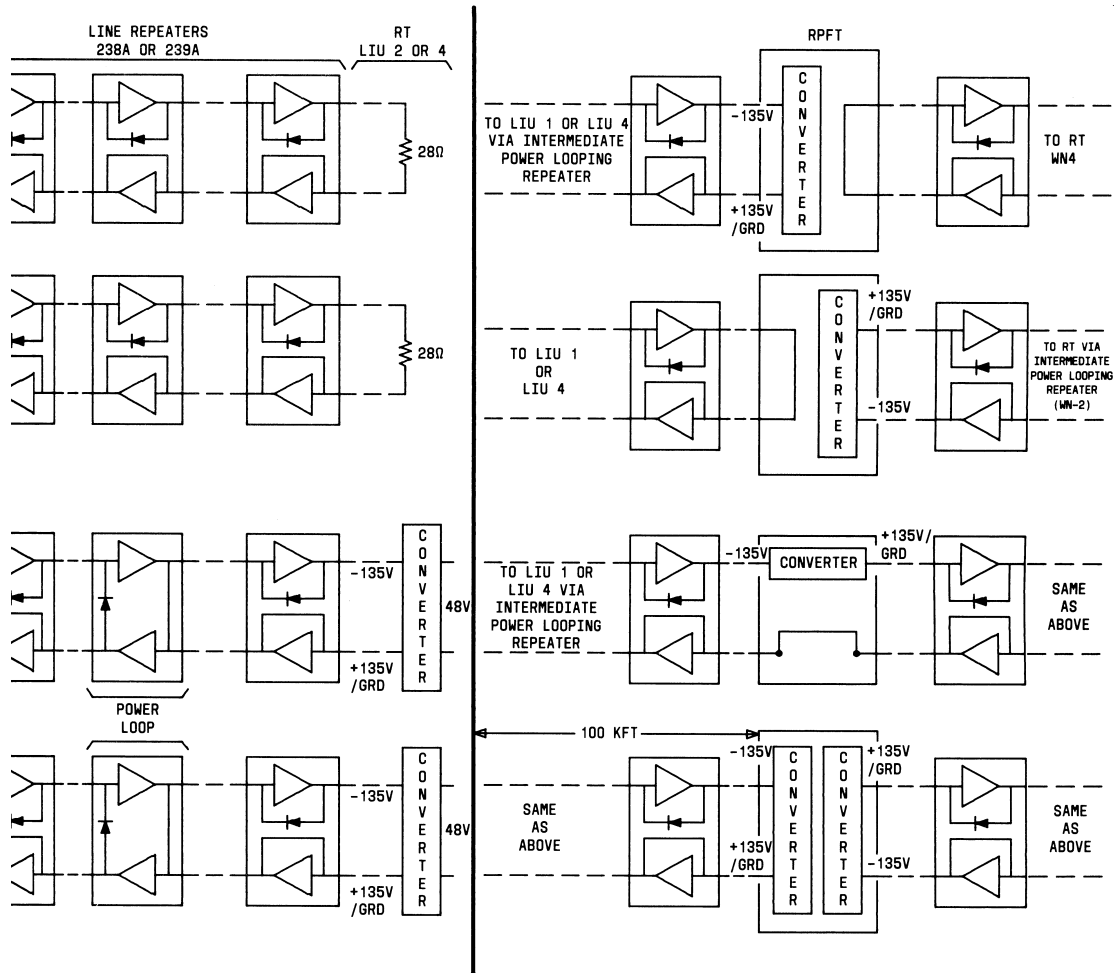


Fig. 1—Typical SLC-96 Powering Applications

SLC-96 Digital Line Preservice Tests

ISS 2, SECTION 363-202-215

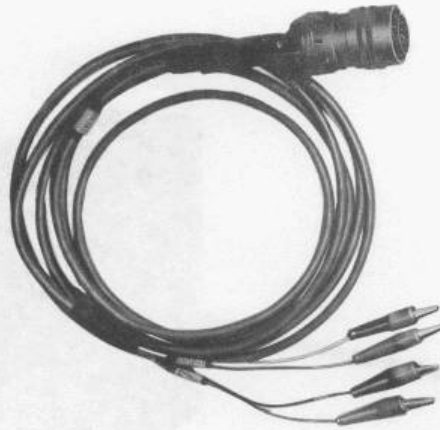


Fig. 2—Sierra 247A-1 Cable Splitting Cord

SLC-96 Digital Line Preservice Tests

SECTION 363-202-215

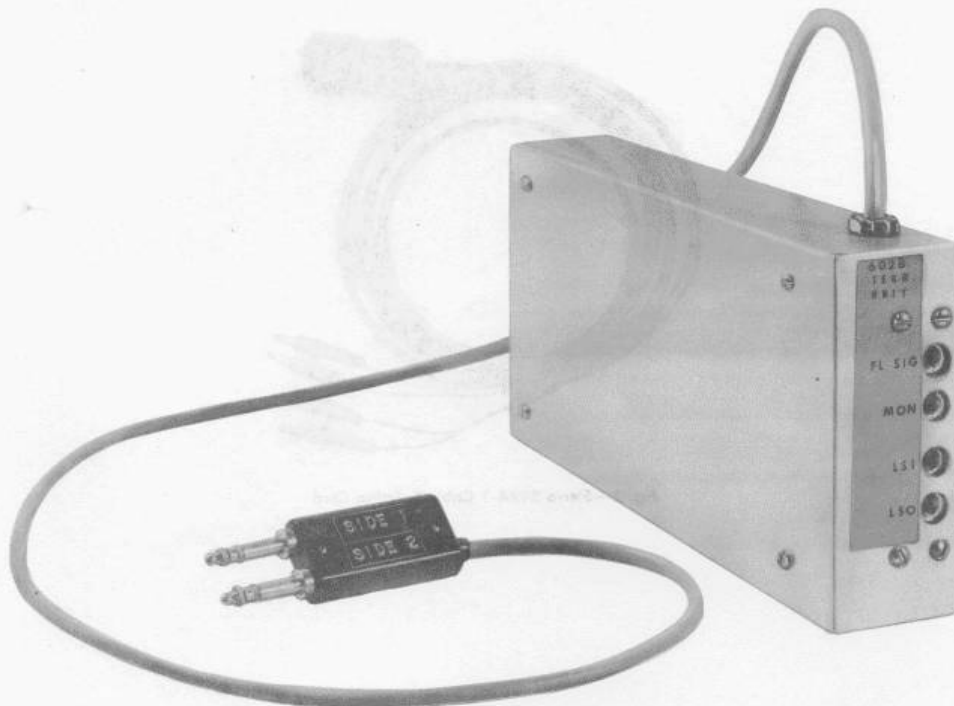


Fig. 3—602B Terminating Unit

SLC-96 Digital Line Preservice Tests

ISS 2, SECTION 363-202-215

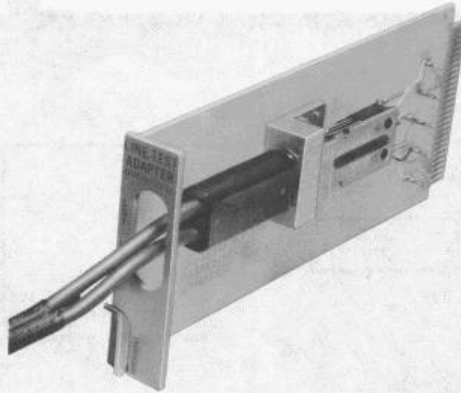


Fig. 4—Line Test Adapter

SLC-96 Digital Line Preservice Tests

SECTION 363-202-215

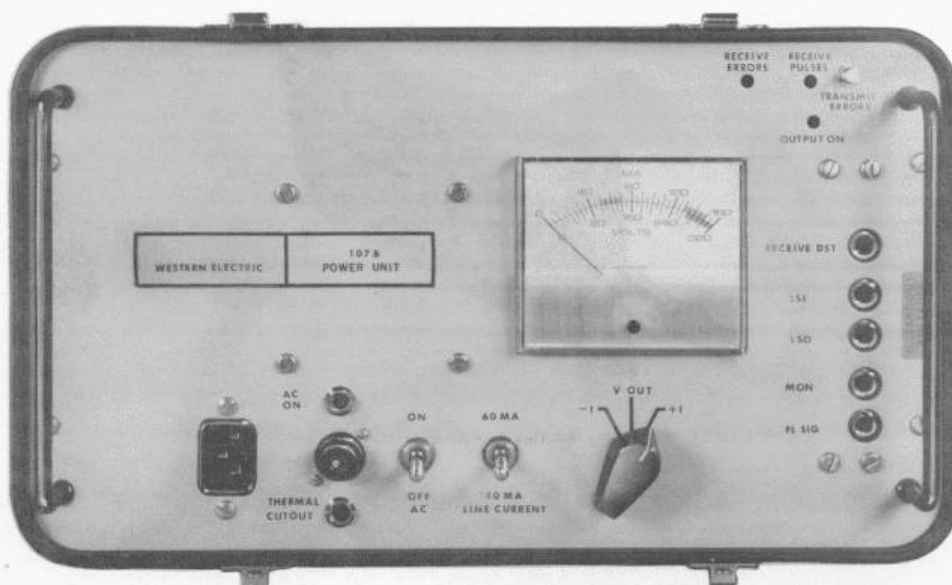


Fig. 5—107B Power Unit

SLC-96 Digital Line Preservice Tests

ISS 2, SECTION 363-202-215

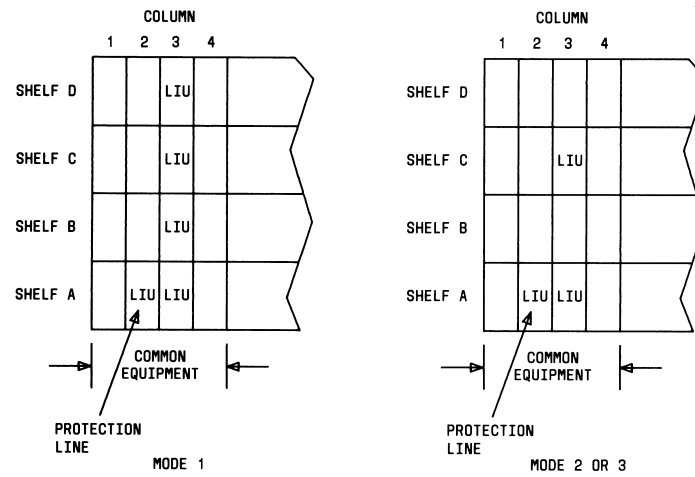


Fig. 6—Positions of LIU Slots in SLC-96 System Channel Banks

SLC-96 Digital Line Preservice Tests

SECTION 363-202-215

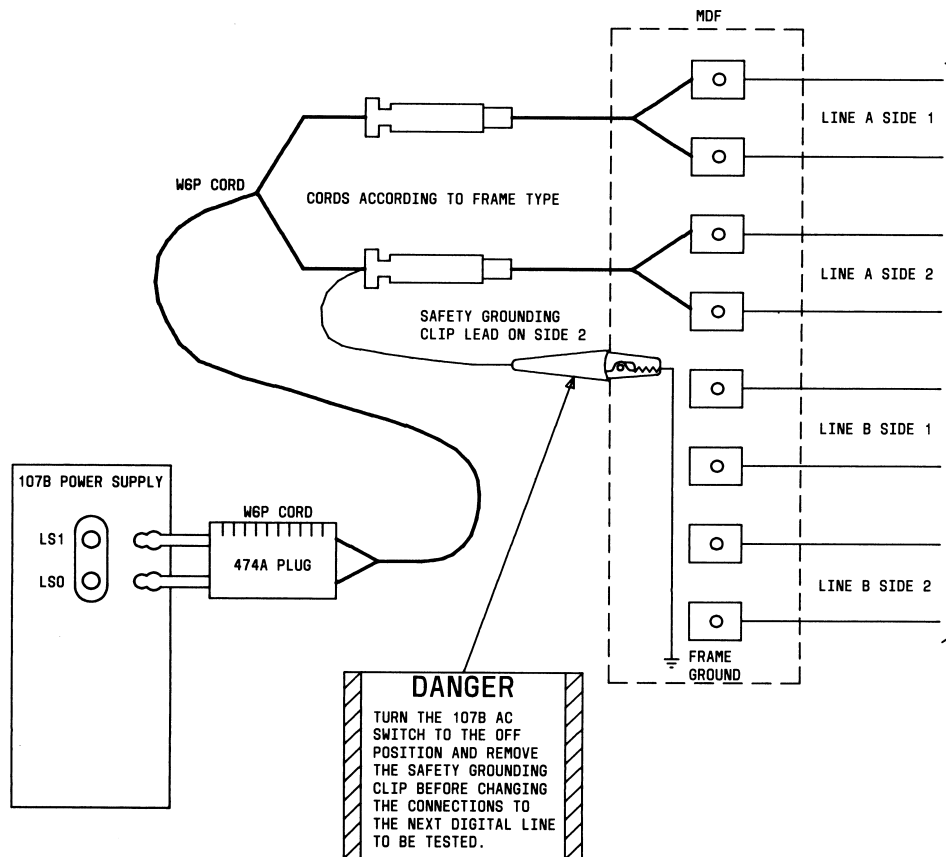


Fig. 7—Test Arrangement Without Use of Line Test Adapter

Motorola High Performance Data Overview

Motorola are being dickheads (as usual) on releasing decent technical info on their new police/fire MDT system, this is what we've found so far...

Motorola High Performance Data

Proposed Solution – Technology Overview

To meet the need for a wide-area wireless data solution, Motorola has proposed the High Performance Data (HPD) technology. The HPD technology offers high bit rates in standard 25 kHz channels within the 700 and 800 MHz bands. To meet the requirements for mission critical data service, HPD offers significant advantages in the key areas of coverage, throughput, and standards.

The HPD Coverage Advantage

Motorola has designed HPD to offer coverage that is approximately equivalent to typical voice coverage. Although this is a very aggressive coverage goal when considering the much faster bit rates that HPD is capable of (96,000 bits per second), Motorola recognizes the value of maximizing coverage to keep site costs as low as possible. For example, if an increase in data speed results in losing half of the range from a given site, then the coverage area is theoretically reduced by 75% and the system would require four times as many base sites to provide coverage that would be equivalent to that of the lower bit rate.

With all things considered equal, physics dictates that for a given channel bandwidth the coverage decreases as the bit rate increases. If the transmit power of base stations and mobiles could be increased, the lost coverage could potentially be recovered; however, the FCC limits transmit power to control noise and interference within any given band. Therefore, power cannot be increased indefinitely to address the issue and other methods of maintaining coverage are required.

To maximize potential coverage, HPD technology implements several key features:

Advanced Modulation Techniques

There is a fundamental tradeoff in communication systems with the use of simple versus more complex transmitters and receivers. Simple hardware can be used in transmitters and receivers to communicate information. However, to increase the bit rate while continuing to use the simpler hardware, more spectrum is required to maintain the same level of coverage performance. Since the spectrum is limited by the bandwidth of the channel, the only option is to suffer coverage degradation. Alternatively, more complex transmitters and receivers can be used to transmit higher bit rates while remaining within the channel's bandwidth limitation. This transition to more and more spectrally efficient transmission techniques requires more complex hardware and is the market trend considering the limited spectrum available today.

In the past, traditional wireless data networks used Frequency Shift Keying (FSK) modulation, which requires simple hardware and is very easy to implement. As an example, Motorola's RD-LAP protocol used a 4-level FSK modulation to achieve a bit rate of 19.2 kbps in a 25 kHz channel. To achieve higher rates than 19.2 kbps, higher order FSK modulations are required such as 8-FSK, or 16-FSK.

The problem with FSK is that the modulation decreases significantly in bandwidth efficiency as the modulation order is increased. With this in mind, HPD was designed using a multilevel Quadrature Amplitude Modulation (QAM) method that achieves a high bit rate using limited bandwidth available. HPD incorporates the use of three QAM formats and automatically adapts between these 3 modulation levels which are QPSK (4-QAM), 16-QAM, and 64-QAM.

Further worth noting, both QAM and QPSK modulation techniques are used by IEEE 802.11 (WiFi), IEEE 802.16 (WiMAX) and 3G (WCDMA/HSDPA) wireless technologies. The use of adaptive modulation allows wireless technologies to optimize throughput, yielding higher throughputs while also covering long distances. The HPD technology is designed to also achieve these critical goals.

Adaptive Modulation

The use of adaptive modulation allows a wireless system to choose the highest order modulation depending on the channel conditions. As the range increases or the channel conditions become more challenging, the modulation automatically adapts down to lower order modulations, such as 16-QAM or QPSK, to maintain coverage. However, in good signal conditions the higher order modulations, 64-QAM or 16-QAM, are used for increased throughput. With the use of adaptive modulation, the system is enabled to better overcome the loss of coverage that is experienced with fixed modulation rate systems.

HPD offers bit rates up to 96,000 bits per second (bps). At such a high rate, coverage will be reduced as physical law dictates; however, HPD has the ability to automatically adapt to lower rates of 64,000 bps (16-QAM) and 32,000 bps (QPSK) as required to insure that coverage is extended into weaker signal areas.

Advanced Forward Error Correction

Channel coding is the best method for transmitting information with fewer errors in weak signal environments. Stronger Forward Error Correction (FEC) coding has the ability to extend coverage beyond the ability of a weaker code. In the past, common codes such as Reed-Solomon, Trellis, and Viterbi have been used as methods for achieving FEC. In 1993, a major advancement in coding, internationally known as Turbo coding, was introduced. Turbo coding enables data communications to come very close to the theoretical limits of a channel, offering significant benefit in coverage performance.

HPD incorporates Turbo coding as a state-of-the-art method for achieving forward error correction. In weaker signal areas where receive errors tend to be the highest, this strong FEC method offers the potential of correcting errors that would otherwise have been uncorrectable with weaker algorithms. Thus, the HPD method enables potential coverage in areas that would have failed due to excessive errors.

Diversity Receive Capability

The standard HPD configuration supports two receive paths on each base station to mitigate fading effects that are common to RF environments. With this approach, two receive antennas are used to capture signals from two spatially different locations on the same tower at a given base site. If one antenna experiences a deep fade but the other captures signal with reasonable quality, the received signal can still be successfully decoded. This method has been proven to provide significant coverage benefits in non-line-of-sight coverage areas.

Efficient Retry Method

It is a known fact that larger messages have a lower probability of being successfully received in comparison to shorter messages. When a message transmission fails in many systems, the entire message is retransmitted and there is no reduction in message size. HPD offers a retry method that retransmits only the portions of a message that have errors rather than retransmitting the entire message. Using this approach, the retried message will be smaller. This approach offers a higher probability of a message being received and ultimately results in improved coverage and throughput.

This method, known as Selective Automatic Repeat Request (SARQ), has been implemented in HPD and is also the method approved by APCO in the P25 wireless data standard.

High-Speed Vehicle Support

In mission critical systems, the ability to support data communications with vehicles moving at high rates of speed is mandatory. With this requirement in mind, HPD was designed to maintain data integrity and reliability at vehicle speeds up to 120 miles per hour.

Non-Line-of-Sight Operation

The HPD offering incorporates the use of a land mobile radio variant of Orthogonal Frequency Division Multiplexing (OFDM) as a critical performance enhancing technology. As the symbol rate for a given channel bandwidth increases, the performance degradation due to multipath delay spread also increases. In the mobile environment, the transmitted signals take many different paths before arriving at a receiver. These paths include reflections off of buildings, cars, mountains, and many other objects. This is referred to as multi-path. Because multiple reflections of the transmitted signal arrive at the receiver at different times, this results in intersymbol interference (or signals "walking on top of each other") which the receiver many times cannot sort out. As the symbol rate increases, multipath interference becomes a greater concern and results in significant coverage loss if not effectively mitigated. OFDM is a well-known technique for combating multipath that has only recently become practical for commercial applications.

OFDM has recently provided significant performance improvements in the wireless LAN market for the 802.11a standard as opposed to the single-carrier direct sequence CDMA physical layer of 802.11b. OFDM can provide the same benefits to wide-area land mobile radio networks as it does for the local-area networks. The basic idea of OFDM is to divide the available channel (25 kHz in this case of HPD) into many subchannels. Rather than transmit data using a single frequency carrier, each sub-channel has a sub-carrier that transmits a significantly lower symbol rate signal. In essence, the transmitted signal is a collection of many lower rate signals that when combined together in the receiver result in a high data rate. Using this OFDM method, the multipath effect is mitigated through the transmission of the slower symbol rates on the sub-carriers.

In short, OFDM is a robust and efficient method for providing non-line-of-sight wireless access in the HPD system. The straightforward way it combats multipath, the high spectral efficiency it provides, and the multiple access efficiency it enables are well suited for providing higher data rates to multiple users without significant coverage penalties.

Improved Receive Sensitivity

In the digital modulation world, detection is the process by which a receiver attempts to determine what information was actually transmitted. For FSK modulation, a simple non-coherent receiver is typically used because the detection process makes decisions based on one dimension, which are shifts in frequency. For QAM modulation, a more complex coherent receiver is used in the detection process to make decisions based on two dimensions, amplitude and phase. Adding another dimension to the process further improves the sensitivity of the receiver which results in increased coverage performance.

Along with the use of QAM modulation, HPD uses coherent modulation methods that bring this added coverage advantage.

Efficient Frequency Reuse

HPD is designed to allow the reuse of frequencies to cover large geographic areas. HPD can be deployed in a cellular-like fashion using as few as 7 channels in a repeating pattern. This gives HPD the flexibility to be deployed over small city areas, large counties, or even state-wide regions using only 7 channels to achieve the required coverage.

Transmitted Power Control

HPD has implemented a method for automatic adjustment of transmit power by mobile units. This enables the mobile units to achieve the required quality of transmitted signal using the minimum required radiated power. Transmitter power control helps to minimize interference levels within the channel, thereby enabling coverage benefits through interference reduction.

For the coverage advantage, HPD implements several technological advancements that position HPD as a highly reliable wide-area wireless technology that offers coverage equivalent to Project 25 voice and data coverage, however, at significantly higher bit rates.

The HPD Throughput Advantage

Motorola's objective is to satisfy two conflicting goals, which are maximizing coverage and maximizing throughput. The actual realized throughput and capacity limits in any given system will be a factor of several variables. Such variables include site density, load distribution across system resources, service area reliability, antenna system design, application profiles, full/half-duplex device operation, and more. Because there are so many variables that define the throughput and ultimate capacity of a system, Motorola would be amiss to state such levels without a complete system design in place. However, Motorola has invested significant resources in developing the HPD technology to insure that greater throughput levels are achieved in any design scenario.

To maximize throughput, some of the key features offered by HPD include:

Fastest Over-the-Air Rate

HPD offers a maximum bit rate of 96,000 bits per second, the fastest rate commercially available in 25 kHz channel bandwidths and a rate that only Motorola has achieved to date. Even at the lower rates of 64,000 and 32,000 bits per second, HPD offers significant speed advantages over many competitive offerings. Motorola anticipates the average channel bit rate to exceed 64,000 bits per second in most implementations.

Adaptive Coding

Although FEC coding is necessary to achieve coverage goals, FEC comes at a price in the form of overhead bits in each data transmission. To minimize the impact of this overhead, HPD includes a methodology for controlling the amount of overhead used for forward error correction. For the strongest error correcting capability in weaker signal areas or for critical portions of the data stream, HPD automatically varies FEC coding rates between 1/2 and 2/3 as required by current channel conditions. With less FEC overhead, user data throughput is increased; however, if more FEC strength is required to deliver a message, HPD is able to make the adjustment to prevent further retries of a message, which also conserves channel capacity.

Advanced Multi-Access

HPD provides an extremely efficient method for supporting multiple users on a single channel. The HPD approach uses a reservation method to prevent users from transmitting messages simultaneously which result in failed transmissions and, ultimately, wasted channel capacity.

The HPD method implements a reservation based method using slotted-Aloha for controlling access to the inbound channel. Using this method, the transmission of data, acknowledgements, and even retries occur in reserved time slots so that there is no threat of collision. Small time slots are provided for requesting access to the channel, or in other words, making the reservation. These smaller time slots are the only time that contention (or collisions of messages) can occur. Overall, channel access efficiency is greatly improved which increases the potential data throughput on a channel.

Efficient Retry Method

HPD's approach to retries also enhances throughput capability. If retried messages are smaller and contain only the portions of the original message that fail, then the channel resources are not burdened with repeat data that has been successfully received. In this regard, more of the channel is freed up to support other data and ultimately the channel capacity is improved. In many systems, retransmissions include the entire message and there is no capacity benefit.

From a user perspective, response times are often longer when operating in weaker signal areas where retries are common. The time between retransmissions of messages often varies from 2 to 4 or more seconds in many deployed wireless systems. With HPD, the average time between retries is on the order of 500 milliseconds, resulting in faster response times even in fringe areas of coverage.

Data Optimized

HPD has been optimized as a narrowband packet switched data service. In most systems supporting voice and data services over the same channel space, voice conversations are typically given priority while data transmissions are queued for future delivery. As voice traffic increases in these systems, data throughput decreases and can be severely limited during peak hours of operation. HPD is dedicated to data service and unaffected by voice traffic so that mission critical data transmissions are prioritized at all times and data throughput potential is not compromised.

Full-Duplex Device Operation

HPD supports full-duplex device operation which enables the transmission and reception of data simultaneously. With full-duplex capability, the modem is able to send multiple data messages while waiting for acknowledgements. In a half-duplex device, the device is transmitting, receiving, or switching between transmit and receive. As such, the throughput to a half-duplex device is less than that available to a full-duplex unit.

With the full-duplex capability built into HPD modems and the way HPD automatically schedules inbound ACKs and retries, support for common industry standard protocols such as TCP and HTTP is feasible.

Sliding Window

HPD implements a sliding window protocol that permits a greater amount of channel throughput (70–80%) to be consumed by a single subscriber radio. The result is much greater throughput rates are available to individual users compared to a stop–n–wait protocol, which typically prohibits more than 30% of the channel throughput for a single user. With HPD, channel throughput is not wasted when it is available. However, the channel bandwidth reservation feature ensures that no single user can dominate channel resources when multiple users need to send data simultaneously.

For the throughput advantage, HPD implements several technological advancements that position HPD as an efficient, high-throughput, packet data service for 25 kHz channels in the 700 MHz and 800 MHz bands.

The HPD Standards Advantage

Motorola understands the value of adhering to standards to protect financial investments, achieve interoperability, and to conform to other existing standards in common use. Motorola developed HPD with full consideration of standards and incorporated these key features:

Migratable

TIA902 is the standard defined by public safety users and industry leaders for wideband data in the 700 MHz band. As defined, TIA902 supports channel bandwidths of 50 kHz, 100 kHz, and 150 kHz. In support of this standard, 700 MHz and 800 MHz HPD modems can be software upgraded to the 50 kHz TIA 902 standard. The RF modems represent a large investment in a typical system deployment; thus, this migration path to the 700 MHz standard protects the initial investment.

Scalable

With the software migration from HPD to the TIA902 standard, the modem scales to a much higher performance level. While many HPD features are also contained in the TIA902 standard, there is a significant increase in available data rate. In a 50 kHz channel, TIA902 provides a maximum burst rate of 230,400 bits per second. In the transition from HPD to TIA902, the maximum RF efficiency increases from 3.8 bits per second per hertz to 4.6 bits per second per hertz. With all elements considered the potential throughput more than doubles.

Industry Standard IP Addressing

HPD supports industry standard IP addressing. With IP addressing, there are no proprietary interfaces to be implemented, saving development time and costs. Also, there is no middleware required for the purpose of IP tunneling or "IP enabling" the network.

On the network side of the system, network hosts interface to the HPD system in the same manner as a common network router to send IP datagram's to mobile units. On the mobile client side, the client computer interfaces the HPD modem using the industry standard Point-to-Point Protocol (PPP). The modem interface also utilizes 10BaseT Ethernet as opposed to the slower serial interface commonly used in narrowband networks.

TCP Compatible

Along with the Internet Protocol (IP), the Transmission Control Protocol (TCP) continues to be the best known and most widely deployed protocol used to communicate across interconnected LAN and WAN systems to support both custom and common applications such as electronic mail, terminal emulation, file transfer, and web browsing.

To meet this challenge, several key HPD design features make TCP support feasible. Key features include the ability to send multiple messages while waiting for ACKs (windowing), automatically scheduled ACKs and retries, reduced time between retries, and full-duplex modems.

Depending on the details of the system design, including all of the design variables, a single HPD channel will provide excellent data throughput. With the advancements, efficiencies, enhancements, and standards built into the HPD technology, Motorola is positioning HPD has a standards-based, high-coverage, high-capacity wide area solution for 25 kHz channels.

Customer Network Interface

The Customer Network Interface (CNI) is the network that connects the HPD network and the Customer Enterprise Network (CEN), where the data application servers will reside.

Since the CEN is administered independently from the radio network, Motorola must coordinate the IP address space to be allocated for the different networks. Motorola will provide the IP addresses belonging to the HPD network and will recommend IP addresses to be used for the CEN.

Border routers are used to connect to the CEN to the HPD network. One side of the border router provides an interface with the CEN while the other side of the border router attaches to a peripheral network to interface with the Gateway GPRS Support Node (GGSN) router on the edge of the radio network.

The intermediate network segment connecting the HPD system to the CEN is referred to as a Demilitarized Zone (DMZ). The DMZ functions to provide a separation of addresses in each network, and creates a safe meeting place between the two networks. The addresses inside the DMZ subnet are used only for linking the networks, and are not advertised outside the DMZ boundary. A server or client knows an address to enter the DMZ, but is not exposed to either DMZ subnet addresses or addresses in the target network. The Network Address Translation (NAT) functions (at each network's router) hide the internal addresses of each network from the other. Address assignment and coordination within both the CEN and the DMZ subnets are customer defined; however, due to security and performance considerations Motorola will assign addresses belonging to the HPD system network.

Gateway GPRS Service Node

The Gateway GPRS Support Node (GGSN) is a special purpose router that provides various services in support of HPD data operation. Among those are separation of IP address spaces between the HPD radio system network and external customer networks, DHCP address management, and tunneling of radio system datagrams into and out of customer networks.

The device is used in the HPD system to provide connectivity between the HPD radio system network and other enterprise networks. It is used to "tunnel" datagrams from the enterprise network to the Packet Data Gateway (PDG), which ultimately passes the datagram on to a specified subscriber unit operating on the "closed" Motorola radio network. A GGSN does the following:

- Isolates the Motorola radio network IP address plan from the IP plans of any CENs to which it enables a connection.
- Supports DHCP services.

Packet Data Gateway

The Packet Data Gateway (PDG) is made up of two separate functional elements – a Radio Network Gateway (RNG) and a Packet Data Router (PDR). The PDG interfaces between the GGSN and the Motorola radio network.

Packet Data Router

The PDR interfaces with the GGSN and controls the routing of data messages between the serving RNG and the GGSN. Additionally, the PDR maintains a database of data-capable Subscriber Units (SU).

The PDR provides a packet data "home" for all SUs that have been Home Zone mapped to that zone for data operation. It sends packets to, and receives packets from the RNG. It also operates with the GGSN to terminate the HPD system's IP address space and provide address translation between the HPD system's IP network and external "customer" networks.

The PDR is responsible for managing data context activation and deactivation. That is, the PDR manages the process of establishing data services and connections for all active SUs. It authorizes and approves context activations by validating provisioning from the network management subsystem against the specified request from the SU. The PDR also determines when context deactivation for a SU is needed. Context deactivation may occur for the following reasons:

- Deactivation of context with the GGSN.
- Loss of contact with RNG.
- Change or deletion of SU provisioning information.

Radio Network Gateway

The RNG is the second of two components within the Packet Data Gateway (PDG). This component interfaces between the Packet Data Router (PDR) and the Subscribers in its own zone.

The RNG in a zone provides a link layer termination point for all the sites in that same zone. The sites and the RNG route data packets over the infrastructure links between remote and master sites in the zone. The RNG receives packets from, and sends packets to, any of the PDRs in the system (that is, PDRs in the same or even other zones). The RNG also holds records of all subscriber units currently affiliated with sites in its zone, acting as the Visitor Location Register (VLR) for data.

The RNG maintains a database of context activated SUs registered in its zone, which is based on actual SU location. SU mobility is tracked on a site-by-site basis. Location information is updated via a mobility "push" from the Zone Controller (ZC). Additionally, the RNG queries the ZC's VLR to verify SU location.

The RNG is responsible for processing and routing data messages. Processing entails breaking down the data message and formatting it into message blocks (CAI format) compatible for over-the-air transfer. The RNG then routes to the appropriate destination device (outbound to the site controller and inbound to the PDR). The RNG performs error checking of all inbound messages that SUs have formatted for over-the-air transfer. After processing, the RNG forwards the message to the PDR.

Zone Controller

For data activity, the Zone Controller (ZC) is responsible for managing mobility information. This is the same zone controller that is also used to support voice operations.

The ZC provides mobility information in the form of "mobility pushes" to the PDR component of the PDG. The PDR uses this information to keep the data system in sync with current SU mobility status. Information that the ZC provides indicates an SU's activity with respect to registration, deregistration, site roaming, and zone roaming. Note that mobility "pushes" occur on every ZC mobility update.

Network Management

The Network Management (NM) suite previously defined to support voice operations is the same NM suite used for the HPD portion of the system. Thus, the entire voice and data solution is managed from the same set of NM applications. The suite includes the ability to perform diagnostics, provision subscriber units, monitor system components, obtain statistical information, configure and control network elements, and monitor system faults.

Mobile Subscriber Unit

Motorola has proposed the HPD 1000 radio modem as the mobile subscriber unit for wireless data services. The HPD 1000 combines the radio and modem function into a single device.

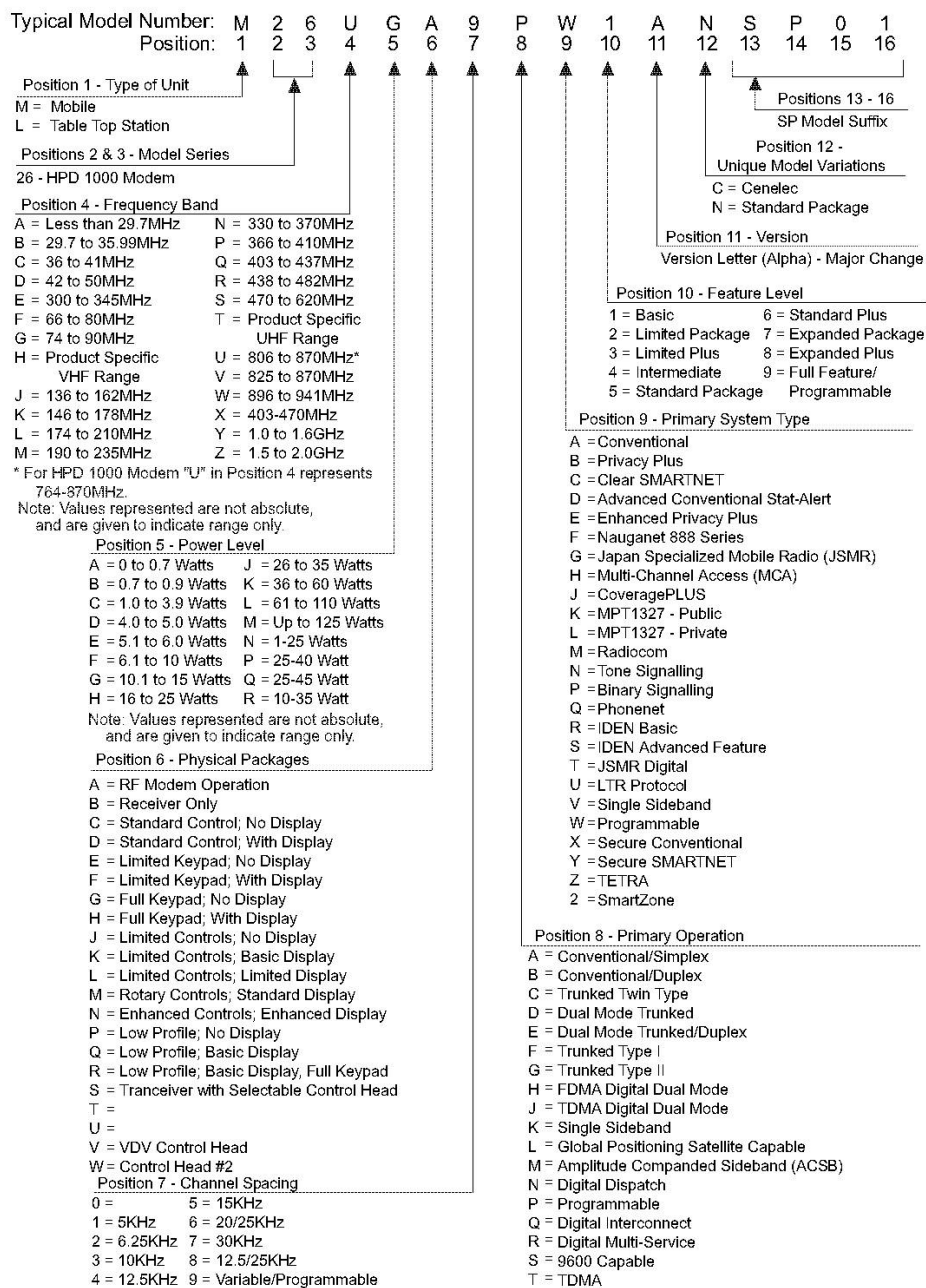
The HPD 1000 supports the mobile computing device through an industry standard PPP connection, which the application will use to exchange IP datagrams with the application server within the customer enterprise network. The PPP connection is physically supported via USB 2.0 connection. Alternatively, an Ethernet connection is available on the HPD 1000 to support a PPP over Ethernet (PPPoE) connection.

To initiate service on the HPD network, the mobile registers for packet data service through a process known as context activation. This process is always triggered from the subscriber-end of the system when the user begins a data session.

The HPD 1000 is a full-duplex device that includes the full HPD feature set, including adaptive modulation, forward error correction, interleaving, selective ARQ, adaptive FEC code rates, reservation-based slotted-Aloha contention control, a land mobile variant of OFDM, and more.

Programming Software: ASTRO 25 Mobile CPS R12.00.00 & TUNER R05.04.00
(or higher - new versions can't read older FLASHports)
Programming Cable: HKN6180 (RS232), HKN6177A, HKN6178A (USB)

Mobile Radio Model Numbering Scheme



2.1.2 Wiring Diagrams

Figure 2-3 shows the modem wiring diagram. Use the diagram when planning the installation.

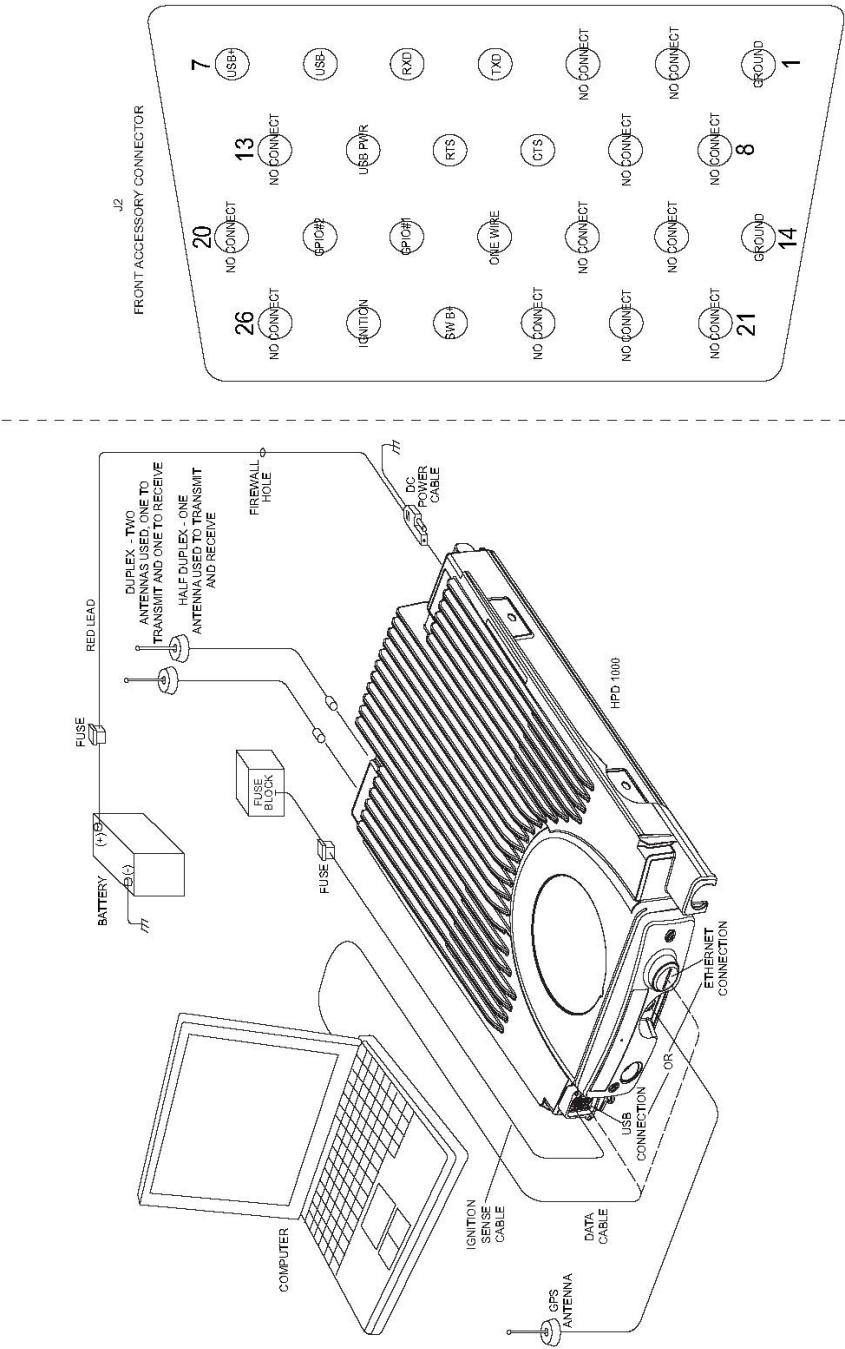


Figure 2-3. Modem Installation

GBPPR RAGEMASTER Experiments

RAGEMASTER – ANT Product Data (NSA)

Capabilities

RF retro-reflector which provides an enhanced radar cross-section for VAGRANT (computer monitor) collection. It's concealed in a standard computer Video Graphics Array (VGA) cable between the video card and video monitor. It's typically installed under the (fake?) ferrite bead on the video cable.

RAGEMASTER provides a target for RF flooding and allows for easier collection of the target monitor's analog video signal. The current RAGEMASTER unit taps the **red** video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.

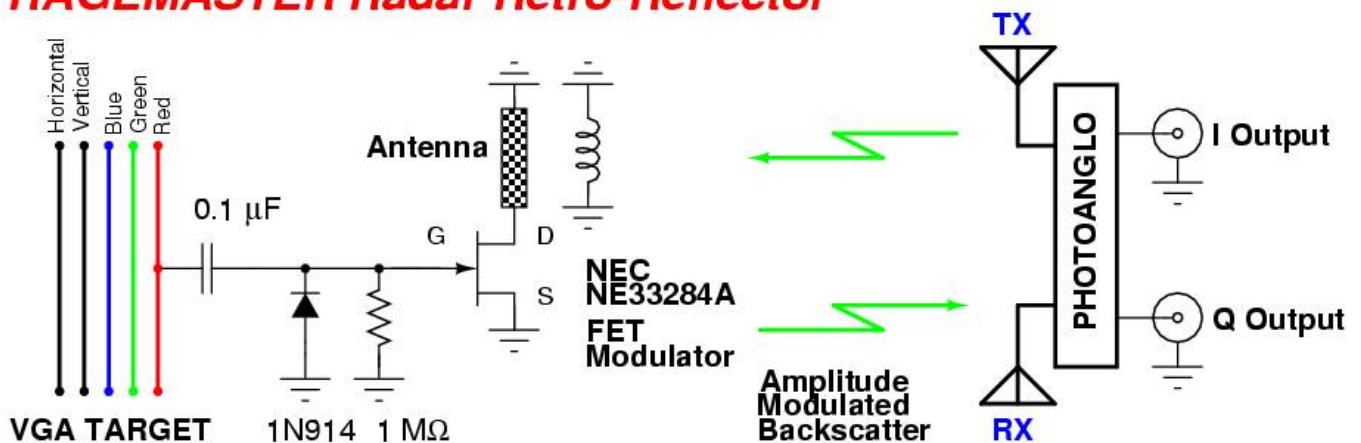
Concept of Operation

The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically a LCD. When the RAGEMASTER is illuminated by a remote radar unit (CTX4000/PHOTOANGLO), the illuminating signal is modulated with the red video information.

This information is re-radiated (backscatter), where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE.

The processing unit recreates the horizontal and vertical synchronization signals of the targeted monitor, thus allowing Tailored Access Operations (TAO) personnel to see what is displayed on the targeted monitor.

RAGEMASTER Radar Retro-Reflector



Shield on monitor cable is broke into two parts.

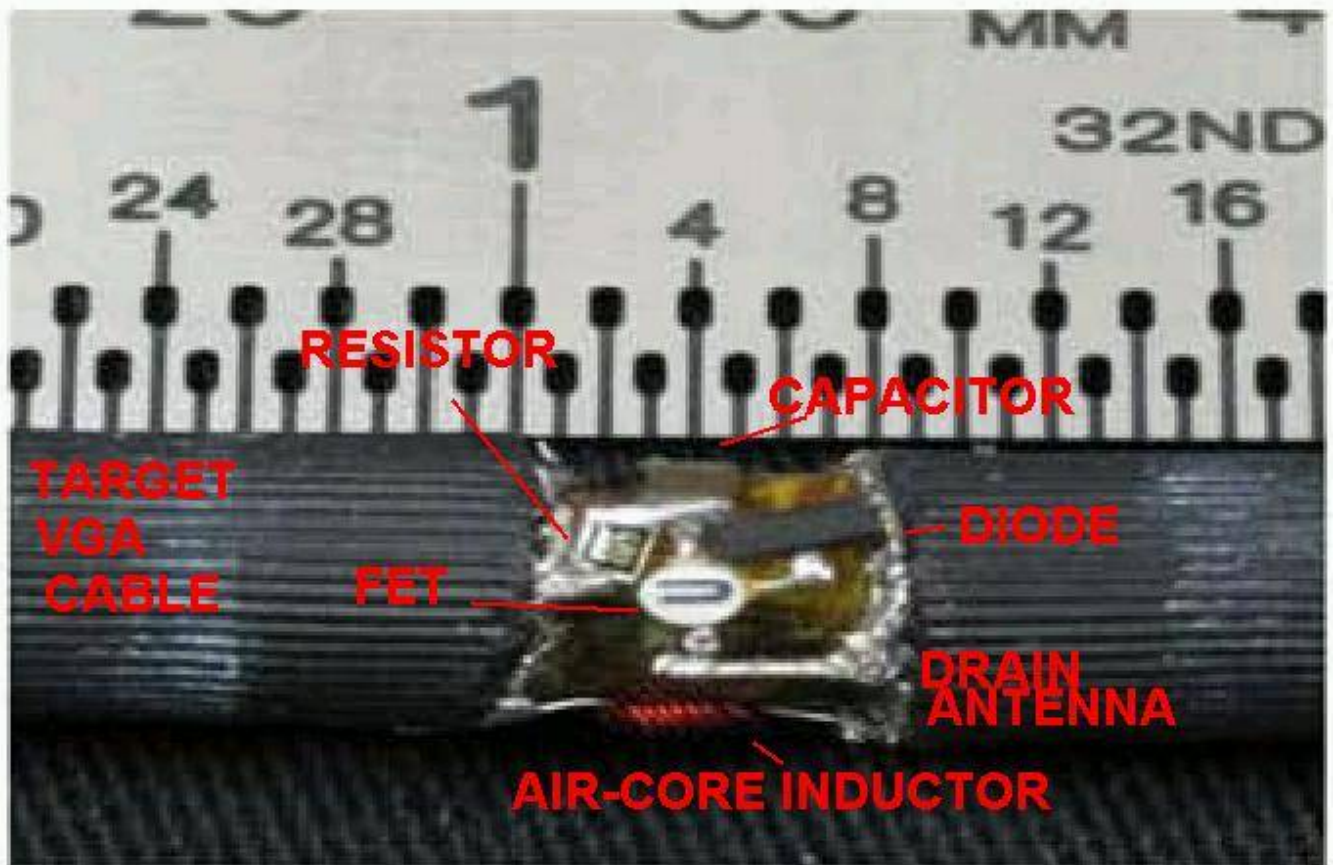
Red air-core inductor in parallel with the FET's drain antenna reconnects the shields and also couples the H&V sync signals via ground "spikes."

The diode is a video DC restore clamp.

Re-insert H&V synchronization with LFS-2 processing unit.

Display received signal on NIGHTWATCH, GOTHAM, or VIEWPLATE.

Pictures & Construction Notes



Overview of an actual NSA RAGEMASTER RF retro-reflector installed in a VGA monitor cable. Taken from the NSA's ANT catalog released by Edward Snowden.

The NEC NE33284A FET is the device with the "U" label.

The yellow film is Kapton tape to prevent anything from shorting out.

The shield on the VGA cable is broken into two pieces. A small 6-turn air-core inductor (enameled red wire) reconnects the shields and also serves to couple the VGA horizontal & vertical synchronization pulses into the backscattered signal via ground "spikes."

A low-frequency spectrum analyzer on the receive processing unit determines the exact horizontal synchronization frequency. The vertical synchronization frequency can be divided down once the horizontal synchronization frequency is known.

Once the horizontal & vertical sync frequencies are known, they are applied to the host display monitor. The sync frequencies need to be exact (phase-locked, ideally) to the target monitor's original frequencies in order to prevent the picture from "rolling."

The final video signal is processed (amplified and low-pass filtered) just like a standard wideband RF signal and applied to the host display monitor's red video input.

The RAGEMASTER implant is just like the TAWDRYYARD implant, except for the clock oscillator and the addition of the diode.



Preparing the VGA video cable for installing of the RAGEMASTER radar retro-reflector.

An approximate 1/4-inch wide piece of the insulation should be carefully removed with a hobby knife.

Real RAGEMASTER radar retro-reflectors are installed under the ferrite bead on the VGA video cable. They are most likely using a fake ferrite bead as the material in a *real* ferrite beads would attenuate the illumination radar.



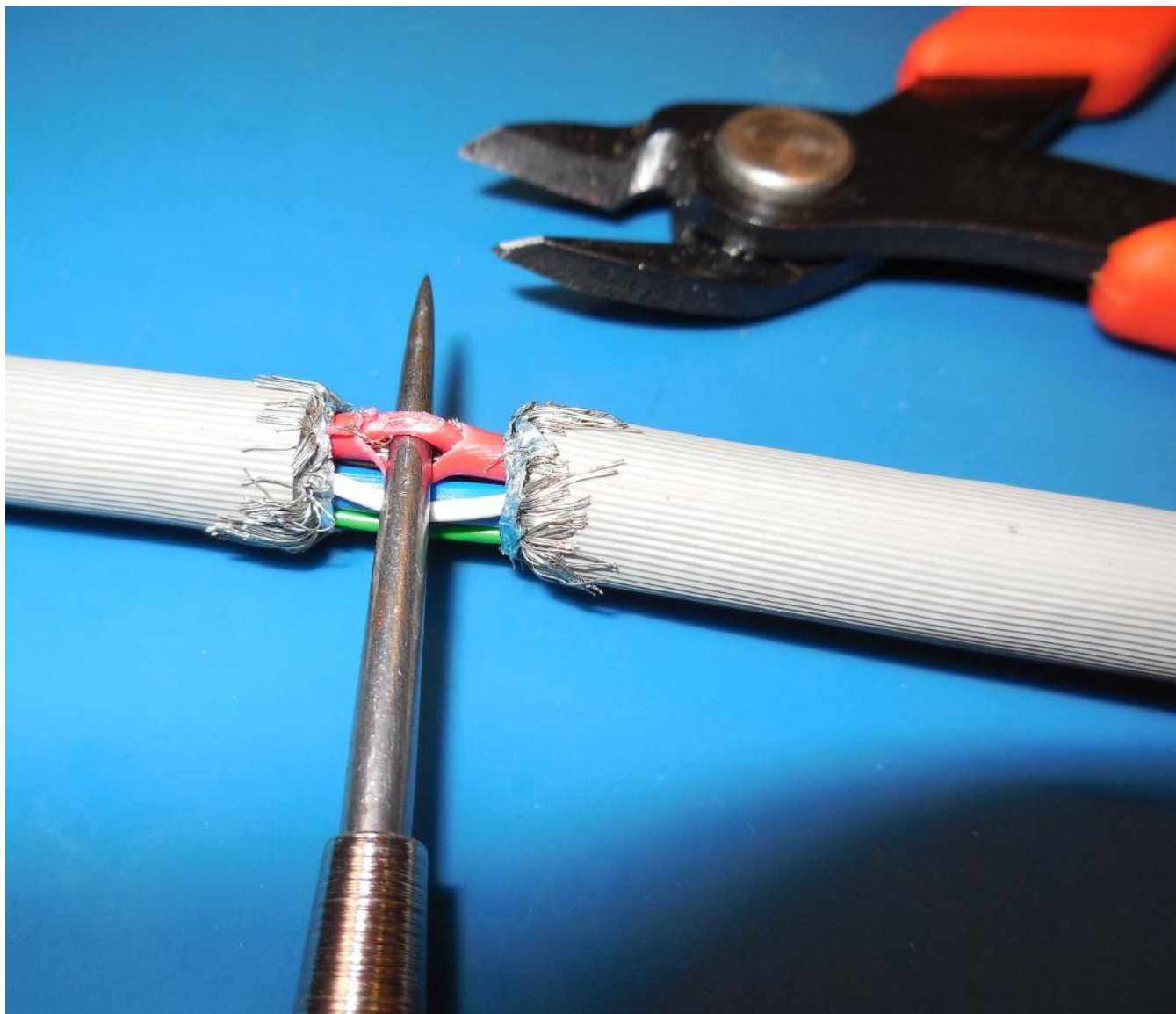
Next you'll want to *very carefully* split the cable's shield into two separate sections. You should verify this with a multimeter.

This is to break up the ground in order to insert an inductor which will help to couple the target monitor's horizontal and vertical synchronization signals into the reflected (backscattered) signal.

The horizontal & vertical synchronization signals determine the final screen resolution (640x480, 800x600, 1024x768, etc.) and the color of the displayed pixel is determined by the value and intensity of the analog red, green, and blue video signals.

The horizontal & vertical synchronization signals are usually standard +5 volt TTL-level pulses, whereas the red, green, and blue video signals are in a continuous (analog) voltage range from 0 VDC (absolutely dark) to +0.7 VDC (maximum brightness).

Each of these three signals controls an electron gun which illuminates the monitor's phosphor pixels a basic color – red, green, or blue. Any other displayed color is the visual mixture of different levels of brightness of those three primary colors.

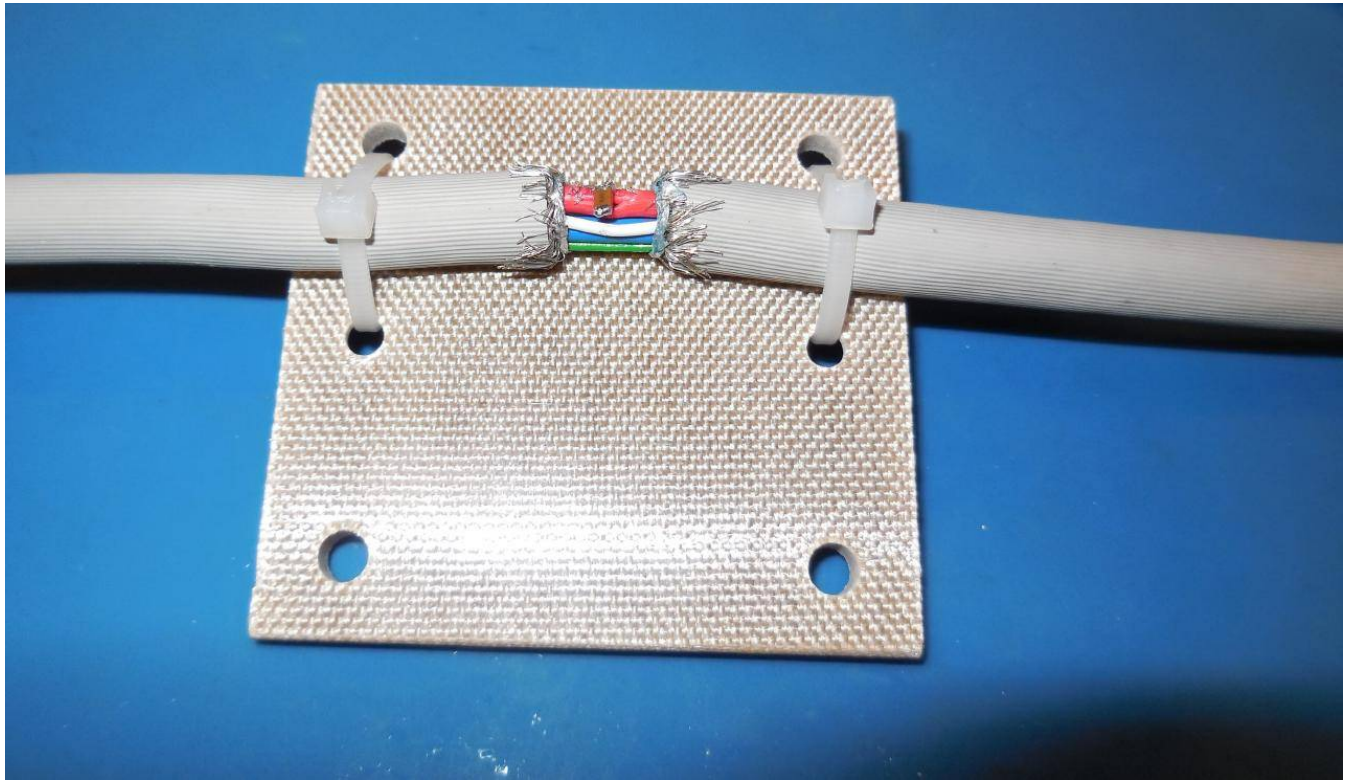


Isolate the red video coaxial cable within the VGA cable bundle.

It's colored red in this particular cable, but that may not always be the case. Double-check with a multimeter to be sure.

Carefully trim away a portion of the outer-shield. Pull out the center conductor and trim away a small portion of its insulation, exposing the center conductor itself. Be sure the center conductor doesn't short against the outer-shield.

In the NSA documents, they state the red video signal provided the best returned signal. I have no idea why this would be the case...



Adding the RAGEMASTER radar retro-reflector components to the target VGA video cable.

It helps to secure (zip-tie) the cable to a small plate, like shown above, to prevent the cable from flopping around when you work on it.

One end of a surface-mount 0.1 μF capacitor is soldered to the red video center conductor.

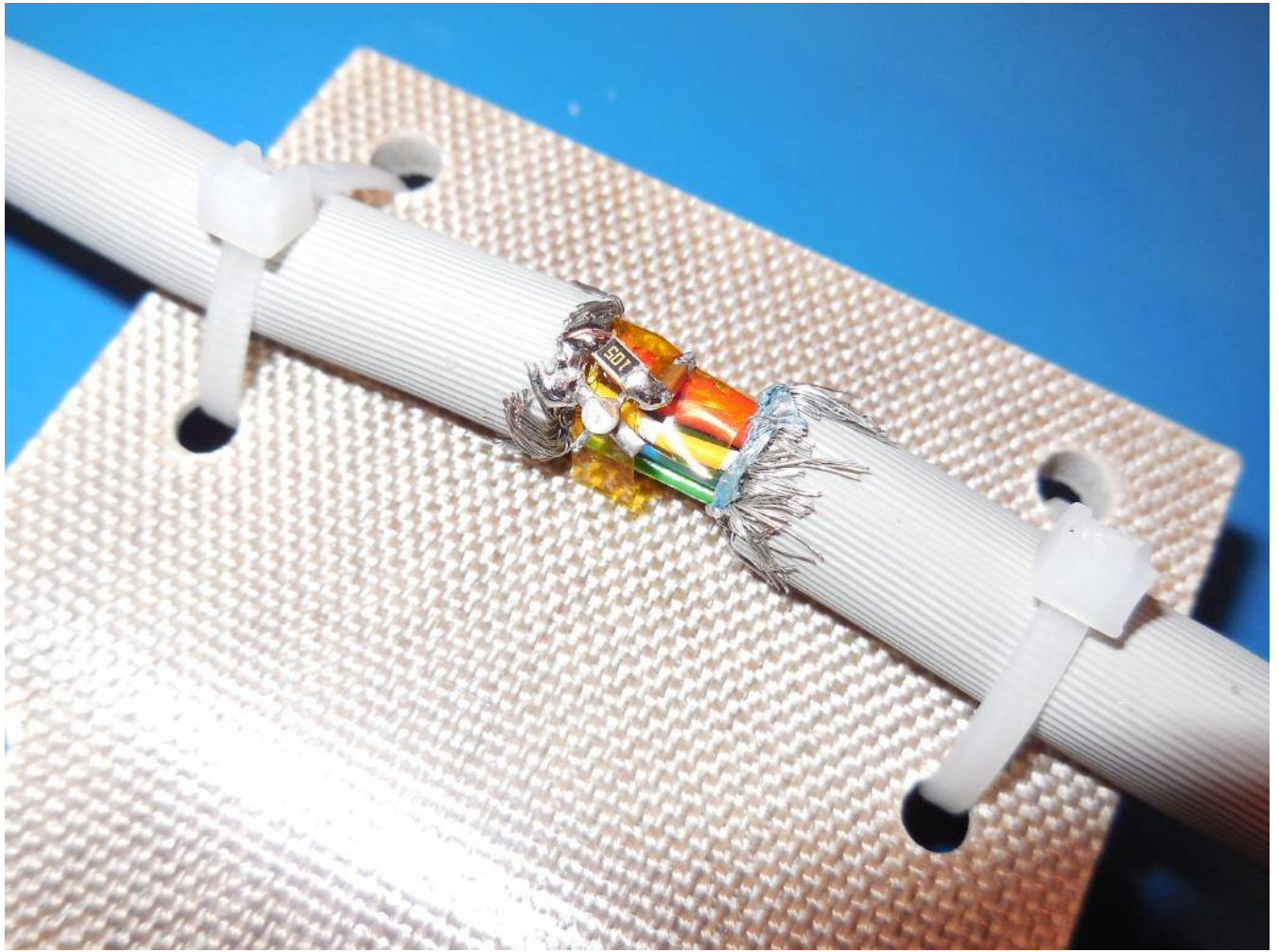
A larger value video coupling capacitor would probably work better, but this application needs to maintain a high-impedance tap to prevent any loading on the low-impedance (75 ohm) target video signal which could reveal your implant.



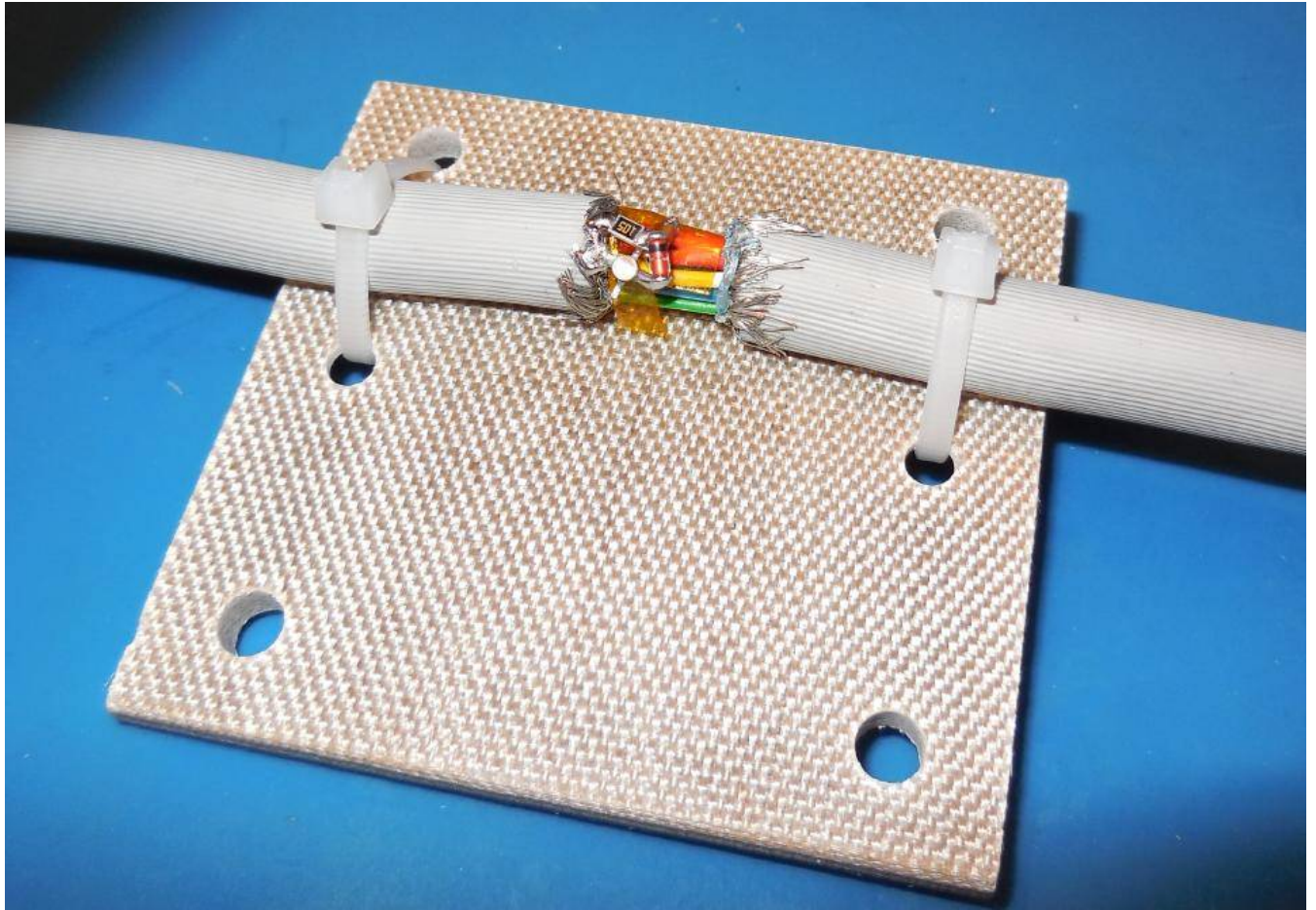
Next, a few pieces of Kapton tape were wrapped around the wire bundle to secure and prevent anything from shorting out.

A Fujitsu FHX35LG FET is used for this retro-reflector instead of the NEC NE33284A shown in the NSA's document.

The gate of the FET is soldered to the other end of the 0.1 μF capacitor and the left source pin is soldered to the left shield (ground) on the VGA video cable.



Next, a 1 megohm gate bias resistor is added from the Fujitsu FHX35LG gate to the left shield (ground).



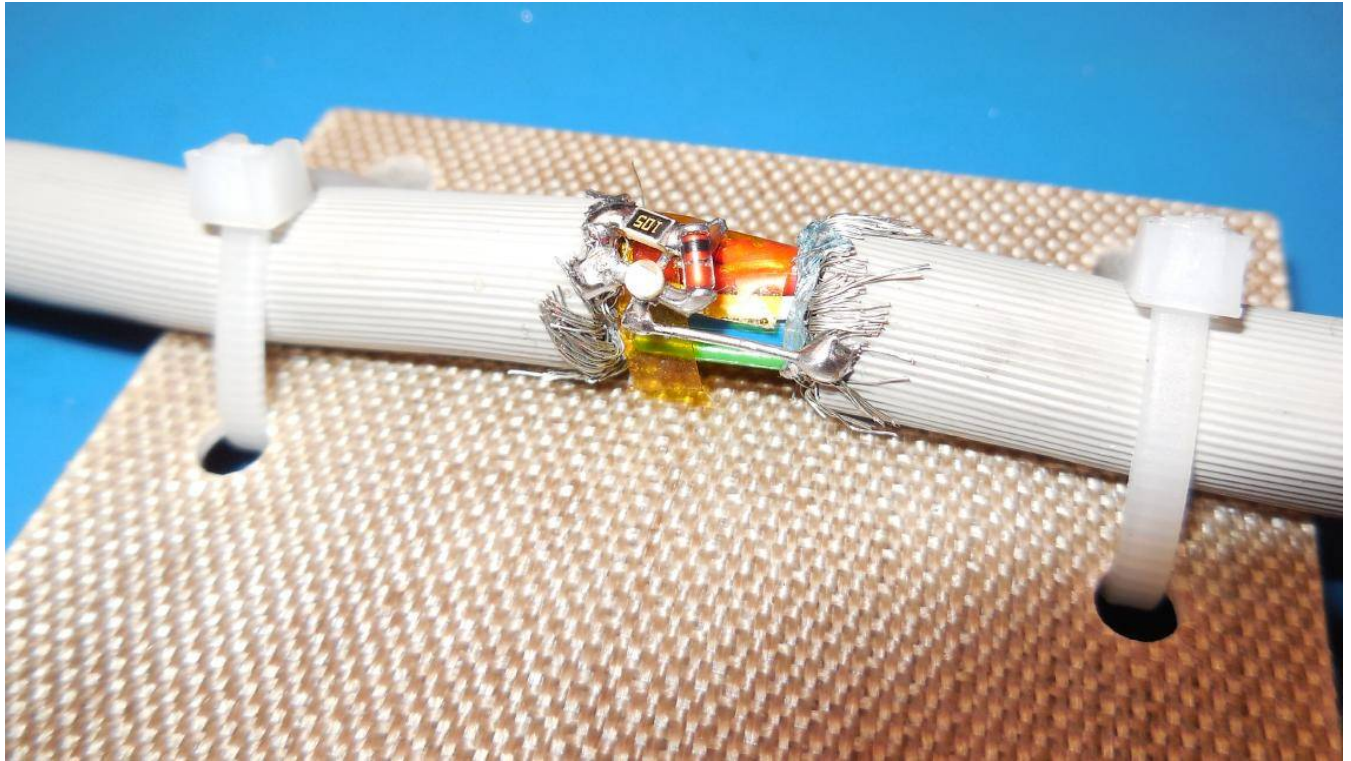
Next, a 1N4148 or similar diode is added from the Fujitsu FHX35LG gate (cathode) to the right source lead, which is at ground potential.

This diode acts like a DC clamp for the video signal.

Analog video signals determine their intensity by their absolute voltages, 0–700 millivolts usually.

When you AC couple the video signal, required to avoid loading the target signal, you lose the "reference" to which the video signal was generated.

This can be recreated by adding a simple diode clamp to readjust the video signal so that it regains its original absolute voltage at known portions within the video signal.



Next, a small piece of wire is added from the the Fujitsu FHX35LG drain to the right shield (ground).

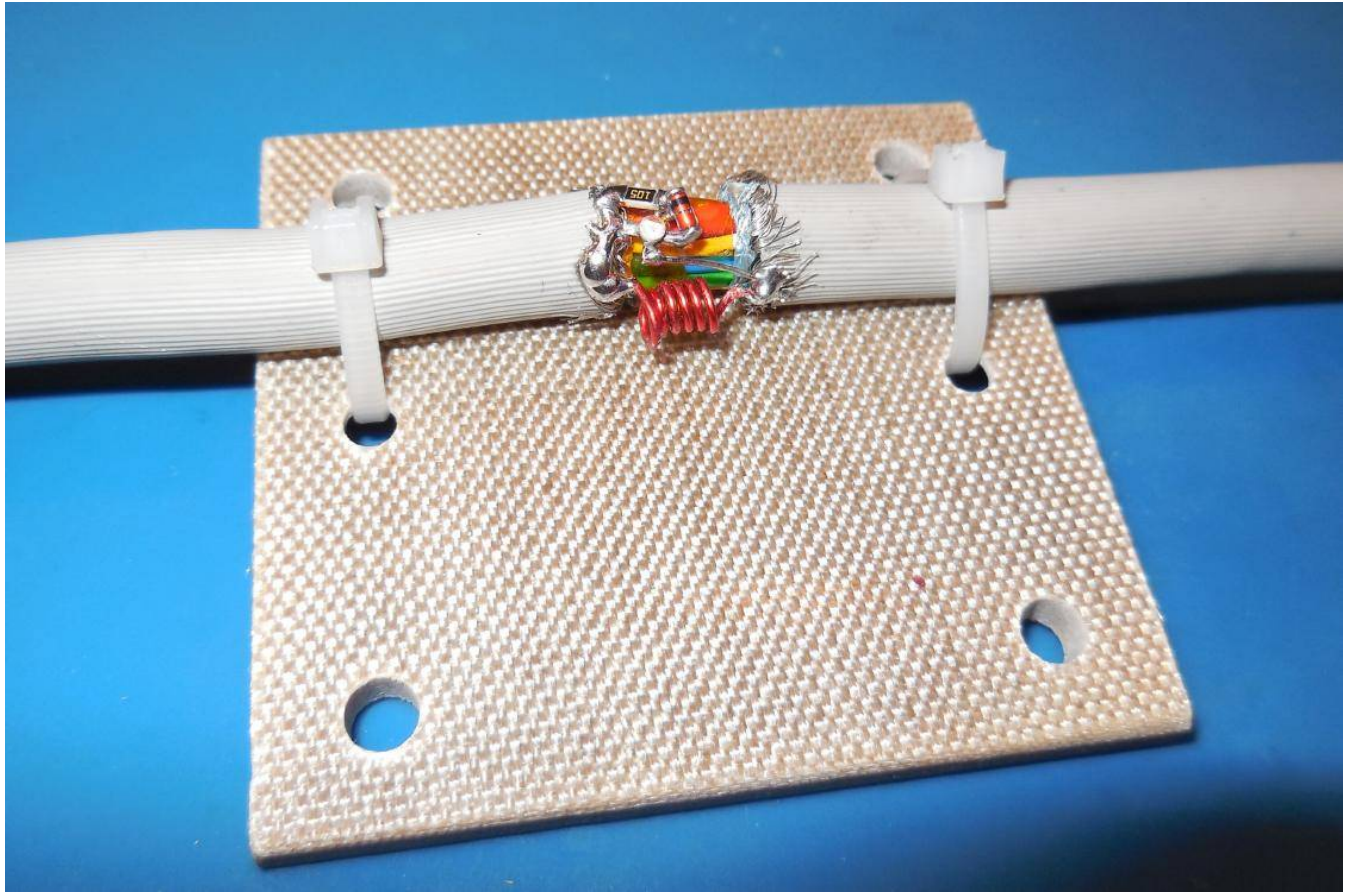
Utilizing the two different grounds generates a differential voltage within the ground system to futher help couple the horizontal and vertical synchronization signals into the backscattered signal.

Here are some example VGA signal timing specifications:

Video Mode	Pixel Clock (MHz)	Horizontal Sync (kHz / Polarity)	Horizontal (in Pixels)				Vertical (in Lines)			
			Active Video	Front Porch	Sync Pulse	Back Porch	Active Video	Front Porch	Sync Pulse	Back Porch
640x480, 60 Hz	25.175	31.469 / Neg	640	16	96	48	480	11	2	31
640x480, 75 Hz	31.500	37.500 / Neg	640	16	96	48	480	11	2	32
640x480, 85 Hz	36.000	43.269 / Neg	640	32	48	112	480	1	3	25
800x600, 75 Hz	49.500	46.875 / Pos	800	16	80	160	600	1	2	21
800x600, 85 Hz	56.250	53.674 / Pos	800	32	64	152	600	1	3	27
1024x768, 75 Hz	78.750	60.023 / Pos	1024	16	96	176	768	1	3	28
1024x768, 85 Hz	94.500	68.677 / Pos	1024	48	96	208	768	1	3	36

On the DB15 VGA connector, the relevant pins are:

<u>DB15 Pin</u>	<u>Description</u>
1	Red Video
6	Red Video Ground
10	Sync Ground
13	Horizontal Sync
14	Vertical Sync

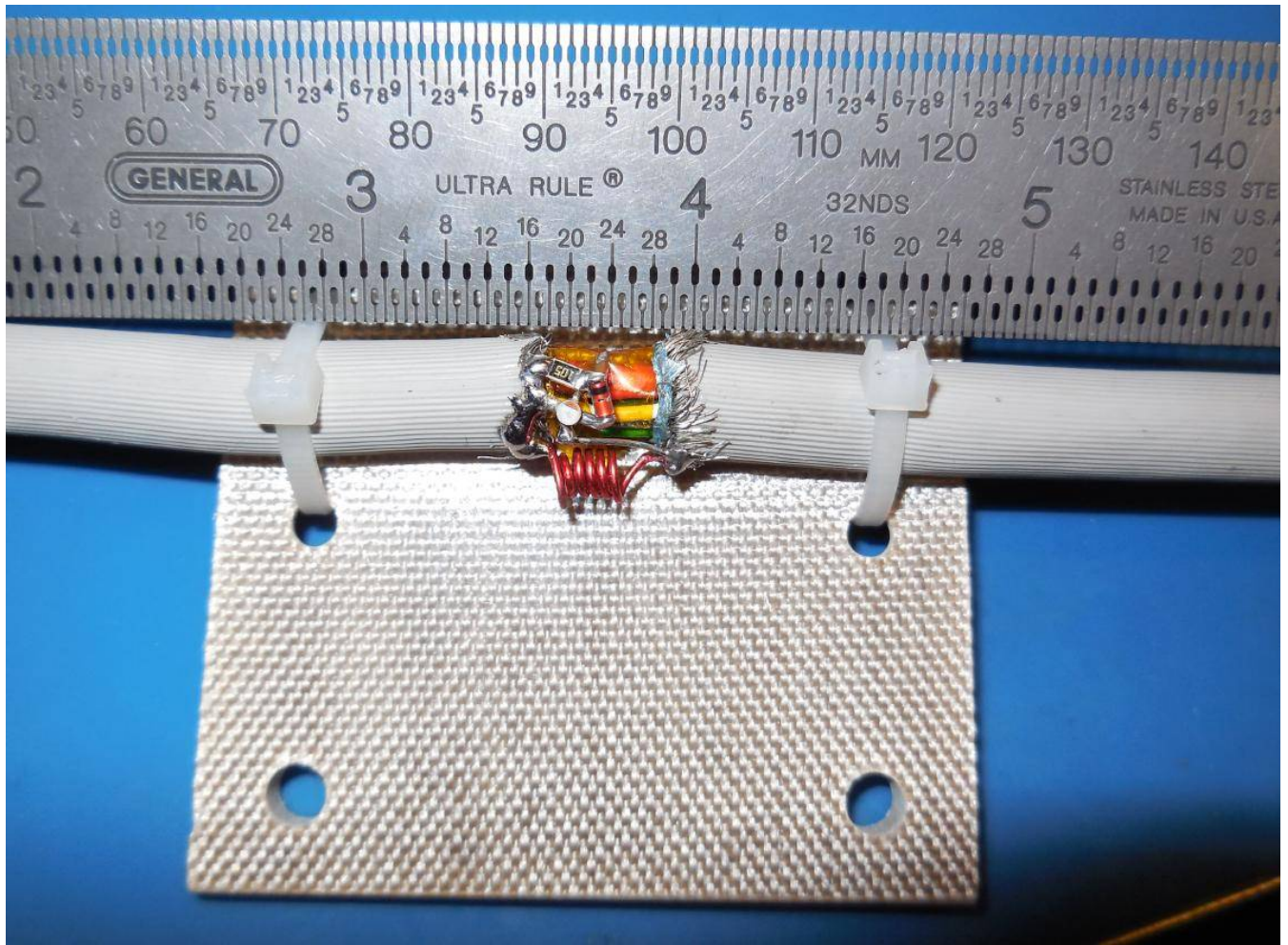


Next, a small 6-turn enameled air-core inductor is added to reconnect the separate (left & right) cable shields.

This is done to create an impedance "bump" within the ground system to help couple the sync signals into the backscattered signal.

Ideally, the air-core inductor should be physically smaller, with 30-gauge wire or so. The exact inductance isn't too critical.

Do be sure the red video signal ground and the cable shield are tied together. Some of the cheaper VGA cables don't have the shield or it's not connected to anything!



Completed experimental RAGEMASTER radar retro-reflector installed in a VGA monitor cable.

Since these radar retro-reflector don't contain a clock, a TAWDRYYARD beacon is often planted to help point the illumination radar (CTX4000/PHOTOANGLO) in the right direction.

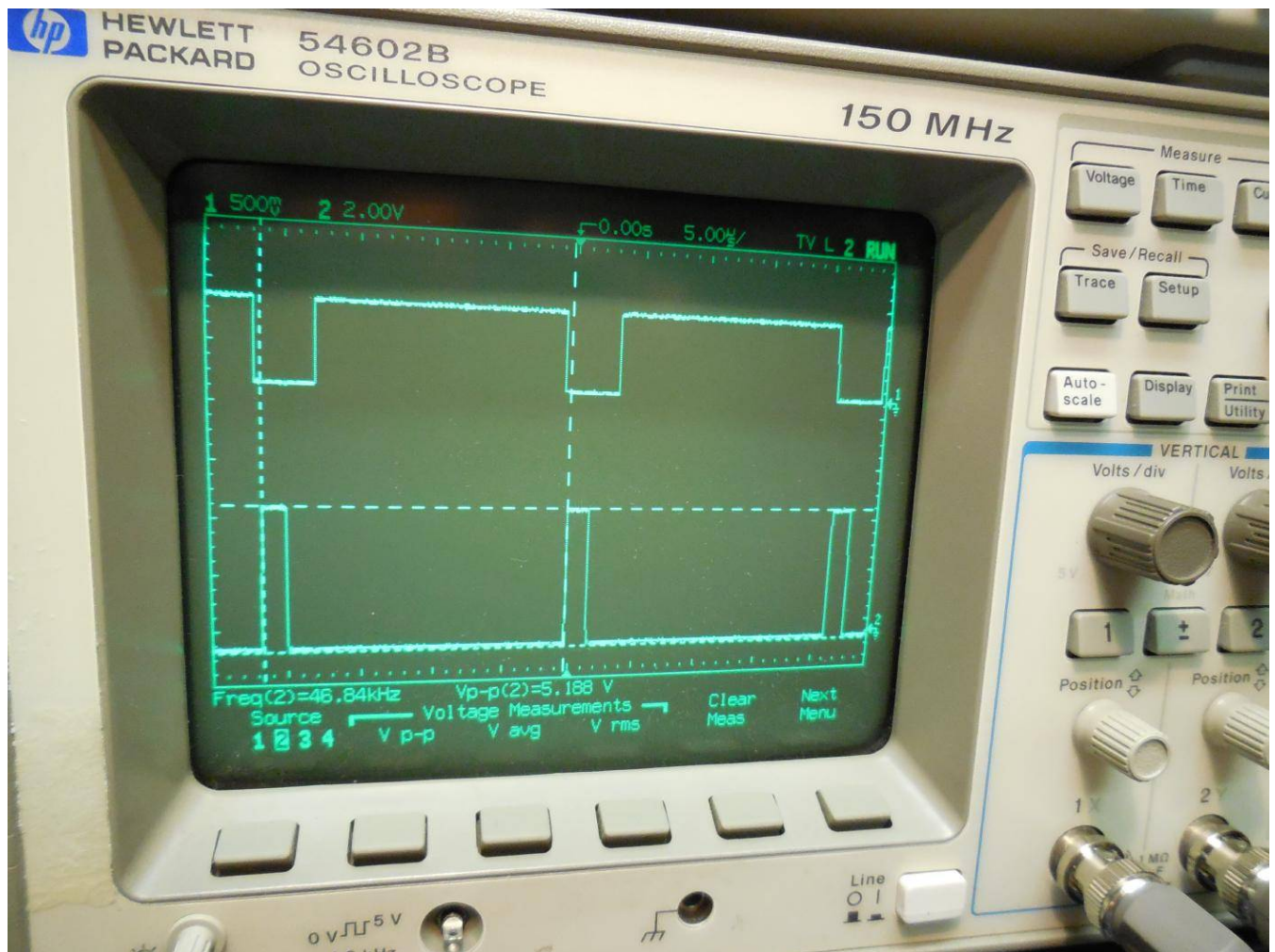
To view the received (backscattered) video signal, you'd need to take the I or Q output from the CTX4000/PHOTOANGLO illumination radar unit and run that through some IF amplification (40 dB or more, probably) and low-pass filtering/post-processing.

You'd then inject this amplified signal into the red video line on your host VGA monitor which is supplying the horizontal & vertical synchronization signals.

You can use a low-frequency spectrum analyzer to monitor the received signal to determine the exact horizontal synchronization frequency your host VGA monitor should be operating at. The proper vertical synchronization frequency can then "divided down" once you find that frequency.

If the horizontal & vertical synchronization frequencies are not the same as the target VGA monitor, the display will "roll" on your host monitor and you won't be able to see anything!

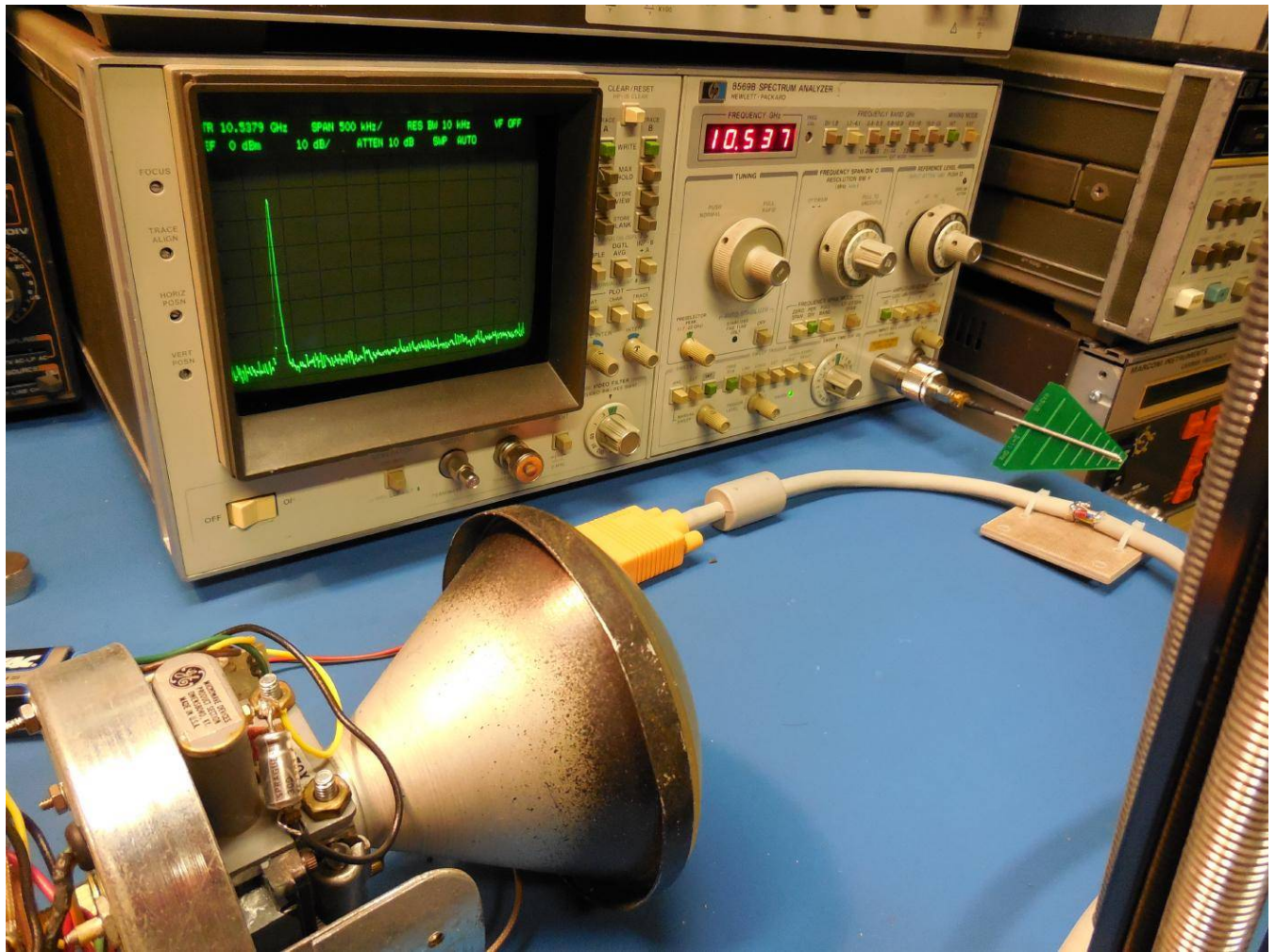
An external tunable sync generator would need to be constructed to tweak the final synchronization frequencies. This is most likely what the NSA's LFS-2 device does.



Oscilloscope view of an "all red" 800 x 600 pixel resolution VGA signal (top trace) which will be used for testing.

It has a horizontal sync frequency (bottom trace) of around 46.84 kHz and a vertical sync frequency (not shown) of 75 Hz.

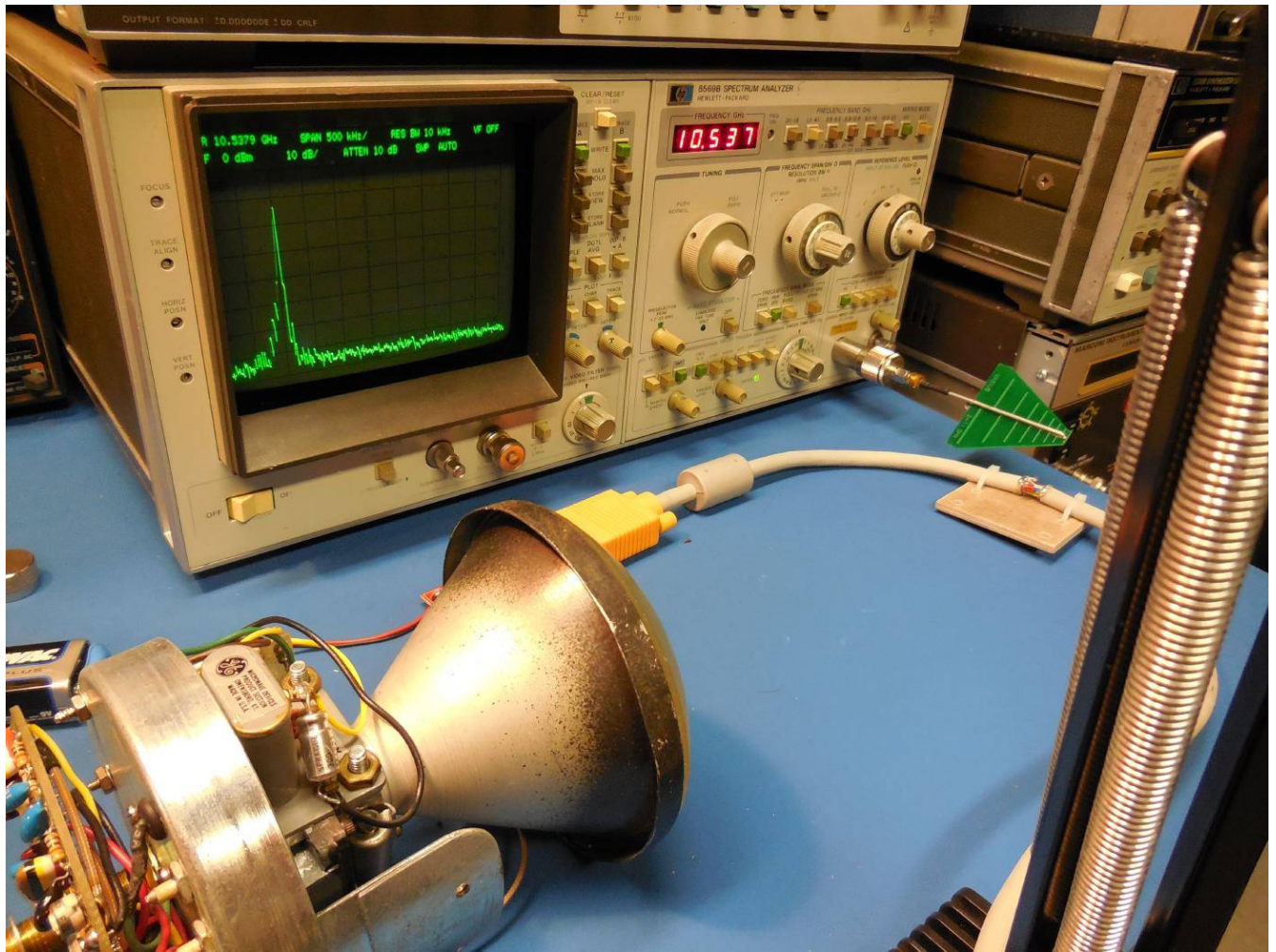
Both the horizontal & vertical sync frequencies are considered "positive" triggered. Some resolutions use negative-edge triggering.



Backscatter video modulation test setup, unmodulated carrier.

On the left, is the unmodulated CW illumination radar, which is a Decatur MV715 RangeMaster operating in the X-band (approximately 10.5 GHz).

The HP8569B spectrum analyzer is showing the unmodulated RF carrier and is centered at 10.537 GHz.



Backscatter video modulation test setup.

The test RAGEMASTER radar retro-reflector installed in a VGA cable is setup inbetween the Decatur MV715 RangeMaster (left) and the spectrum analyzer's RF input (right).

The FHX35LG FET is being (gate) modulated with the red video line of the VGA test signal.

The amplitude modulated backscatter video signal is being received and displayed on the spectrum analyzer.

If you were to AM demodulate the backscattered signal, and apply it to the video input of a monitor operating at the same horizontal & vertical sync frequencies as the target monitor, you'd be able to see what's on the screen – or that's the idea at least...

The target monitor's sync frequencies are also modulated within the backscattered video signal. The horizontal sync frequencies will appear as a series of "spikes" within the video signal on the spectrum analyzer.

You can "hear" the vertical sync frequencies (60/75/85 Hz or so) via the illumination radar's output with a standard audio amplifier and headphones.



RAGEMASTER

ANT Product Data

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

24 Jul 2008

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.



(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

Unit Cost: \$ 30

Status: Operational. Manufactured on an as-needed basis. Contact POC for availability information.

POC: [REDACTED], S32243, [REDACTED], [REDACTED]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108



NIGHTWATCH

ANT Product Data

(TS//SI//REL TO USA,FVEY) NIGHTWATCH is a portable computer with specialized, internal hardware designed to process progressive-scan (non-interlaced) VAGRANT signals.

24 Jul 2008

(U) Capability Summary

(TS//SI//REL TO USA,FVEY) The current implementation of NIGHTWATCH consists of a general-purpose PC inside of a shielded case. The PC has PCI digitizing and clock cards to provide the needed interface and accurate clocking required for video reconstruction. It also has:

- horizontal sync, vertical sync and video outputs to drive an external, multi-sync monitor.
- video input
- spectral analysis up to 150 kHz to provide for indications of horizontal and vertical sync frequencies
- frame capture and forwarding
- PCMCIA cards for program and data storage
- horizontal sync locking to keep the display set on the NIGHTWATCH display.
- frame averaging up to 2^{16} (65536) frames.



(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The video output from an appropriate collection system, such as a CTX4000, PHOTOANGLO, or general-purpose receiver, is connected to the video input on the NIGHTWATCH system. The user, using the appropriate tools either within NIGHTWATCH or externally, determines the horizontal and vertical sync frequencies of the targeted monitor. Once the user matches the proper frequencies, he activates "Sync Lock" and frame averaging to reduce noise and improve readability of the targeted monitor. If warranted, the user then forwards the displayed frames over a network to NSAW, where analysts can look at them for intelligence purposes.

Unit Cost: N/A

Status: This system has reached the end of its service life. All work concerning the NIGHTWATCH system is strictly for maintenance purposes. This system is slated to be replaced by the VIEWPLATE system.

POC: [REDACTED] S32243, [REDACTED] [REDACTED]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

Bonus



This is an actual RF cable assembly taken from a Motorola MSF5000 UHF repeater system used by the Milwaukee police.

End of Issue #122



Any Questions?

Editorial and Rants



REFERRAL/INFRACTION:	Sharp object / weapon possession	TEAM:	Red
----------------------	----------------------------------	-------	-----

CIRCUMSTANCES OF INCIDENT:
 Sean was brought to the office by a staff member who reported that Sean had a sharp object on him in his right pocket. When asked what he had in his pocket he reported he did not have anything. When asked to empty his pockets he refused. After several minutes Sean emptied his pockets. The contents of his pockets included a cell phone, pen cap, and paper clip. The paperclip was bent in a manner that could allow for use as a weapon.

PREVIOUS CORRECTIVE ACTION TAKEN (such as changing student's seat, parent notification and teacher detention):

Any suspected report of HIB must be reported verbally to counselor or administration immediately.

Check reasons for suspected HIB

<input type="checkbox"/> Hurtful teasing	<input type="checkbox"/> Hurtful name calling	<input type="checkbox"/> Insulting Remarks	<input type="checkbox"/> Sending nasty notes
<input type="checkbox"/> Socially excluding	<input type="checkbox"/> Spreading Rumors	<input type="checkbox"/> Stealing	<input type="checkbox"/> Physical behavior
<input type="checkbox"/> Threats	<input type="checkbox"/> Stalking	<input type="checkbox"/> Inappropriate sexual behavior/comments	

DATE/TIME OF ALLEGED HIB INCIDENT: 6/11/14

([reddit.com/r/pics/comments/280x6a/my_friends_little_brother_got_suspended_for](https://www.reddit.com/r/pics/comments/280x6a/my_friends_little_brother_got_suspended_for))

Student suspended for having a "paperclip bent in a manner that could allow for use as a weapon."



Oh shit... Get ready for World War 3!

Change!



#OpenBordersForIsrael

twitter.com/hashtag/OpenBordersForIsrael

A greater influx of impoverished immigrants and refugees, especially from Sub-Saharan Africa, will add to the rich cultural tapestry that underpins Israel. It's time that Israel adopts a much more liberalized immigration and border-security policy.

We've all seen the astonishing social and cultural benefits that Europe and the U.S. have attained through opening the floodgates to immigration and asylum seekers.

In 2011, Sweden alone accepted well over 20,000 asylum seekers. During the same period, out of over 4,500 asylum applications, the Israeli state accepted a grand total of 1!

How can Israel expect to attain the same level of cultural enrichment and vibrancy as Sweden or Norway if it refuses to open its borders?

It's time to make our voice heard: the future of Israel depends on it becoming a multicultural state.

It's a huge transformation for Israel to make and we will be resented by racists for our leading role, but, without that transformation, Israel will not survive.



Saw this on posting recently on /pol/:

"Sweden has fallen! I took this picture when I graduated in Gothenberg the fifth of June... Nuke us now please before it spreads. Cya in nigghalla </3"

Sadly, it looks like there only a handful of Swedes in that picture, on the middle-right.





 The Democrats 
@TheDemocrats



 Follow

Happy Flag Day! pic.twitter.com/I93jQ7ji1e

 Reply  Retweet  Favorite  More



RETWEETS
206

FAVORITES
130



1:04 PM - 14 Jun 2014

Flag media

Democrats celebrate Flag Day... with a non-American flag!

(twitter.com/TheDemocrats/status/477874188687265793/photo/1)